Universidad Autónoma de Puebla

Facultad de Ciencias de la Computación

Sistema Electrónico de Votación

T E S I S

PARA OBTENER EL GRADO DE

Maestro en Ciencias de la Computación

PRESENTA

Lic. María de Lourdes López García

ASESOR

Dr. Miguel Ángel León Chávez

CO-ASESOR

Dr. Francisco Rodríguez Henríquez

Índice

Índice de Figuras ..... *iii*

Introducción *1*

1.1 Descripción del problema *1*
1.2 Objetivo general *4*
1.2 Objetivos específicos *4*
1.3 Metodología *6*
1.4 Estructura del documento *9*

Sistemas de Votación *11*

2.1 Sistema de votación convencional *11*
2.2 Sistemas de votación electrónica *12*
2.3 Sistemas de votación electrónica por Internet *13*

Voto por Correo Postal en México *19*

3.1 Reforma electoral 2005 ..... *19*
3.2 Voto por correo postal *20*

Sistema Electrónico de Votación por Internet (SEVI) *27*

4.1 Modelo de casos de uso *27*
4.2 Modelo de análisis *34*
4.2.1 Caso de uso registro *34*
4.2.2 Caso de uso consultar estado del trámite *35*
4.2.3 Caso de uso votación *36*
4.2.4 Caso de uso generación de resultados *37*
4.2.5 Caso de uso auditar voto *38*
4.2.6 Caso de uso auditar distrito *38*
4.2.7 Caso de uso administración del sistema *39*
4.3 Diagrama de clases *39*
4.4 Seguridad en SEVI *42*

Modelo de Diseño SEVI *43*

5.1 Protocolos de seguridad *44*
5.1.1 Basado en Lin-Hwang-Chang *44*
5.1.1.1 Implementación en SEVI *49*
5.1.2 Protocolo de transmisión segura SSL (Secure Sockets Layer) *52*
5.2 Bases de datos *56*
5.2.1 Diagramas entidad-relación *57*
5.3 Diagrama de clases refinado *61*

Modelo de Implementación y Pruebas SEVI *81*

6.1 Implementación de los casos de uso *85*
6.1.1 Registro *85*
6.1.2 Consultar el estado del trámite *90*
6.1.3 Votación *92*
6.1.4 Generación de resultados *95*
6.1.5 Auditar distrito *97*
6.1.5 Auditar voto *99*
6.2 Modelo de pruebas *101*

Conclusiones *103*

7.1 Trabajo futuro *105*

Libro Sexto del COFIPE *107*

Especificaciones SEVI *125*

B.1 Compilación de los paquetes instalados sobre Linux en cada servidor *126*
B.1.1 OpenSSL 9.8.b *126*
B.1.2 Apache 2.0 ..... *127*
B.1.3 GMP 4.2.1 ..... *128*
B.1.4 Oracle 9i *129*
B.1.5 PHP 5.1.4 ..... *132*
B.2 Código Fuente. SEVI *133*

Índice de Figuras

Fig. 3.1 Procedimiento de votación en el extranjero, modalidad por correo postal *25*
Fig. 4.1 Primera aproximación de funcionalidad de SEVI *28*
Fig. 4.2 Diagrama de casos de uso SEVI *33*
Fig. 4.3 Diagrama de clases SEVI *41*
Fig. 5.1 Diagrama de composición de SEVI *43*
Fig. 5.2 Protocolo de seguridad basado en Lin-Hwang-Chang *50*
Fig. 5.3Protocolo de seguridad basado en Lin-Hwang-Chang, ajustado a la ley electoral (COFIPE) *51*
Fig. 5.4 Secuencia simplificada del handshake de SSL *53*
Fig. 5.5 Pila del protocolo SSL *55*
Fig. 5.6 Diagrama E-R base de datos IFE *57*
Fig. 5.7 Diagrama E-R base de datos SR *58*
Fig. 5.8 Diagrama E-R base de datos SA *59*
Fig. 5.9Diagrama E-R base de datos SV *60*
Fig. 5.10 Diagrama E-R base de datos SC *61*
Fig.5.11 Diagrama de clases refinado caso de uso registro *62*
Fig.5.12 Diagrama de secuencia para el registro del Ciudadano *64*
Fig.5.13 Diagrama de clases refinado consulta estado del trámite *65*
Fig.5.14 Diagrama de secuencia consulta estado del trámite *66*
Fig.5.15 Diagrama de clases refinado caso de uso votación *68*
Fig. 5.16 Diagrama de secuencia votación (parte 1) *69*
Fig. 5.17 Diagrama de secuencia votación (parte 2) *71*
Fig. 5.18 Diagrama de secuencia votación (parte 3) *72*
Fig. 5.19 Diagrama de clases refinado generación de resultados *73*

Fig. 5.20 Diagrama de secuencia generación de resultados 74
Fig. 5.21 Diagrama de secuencia generación de resultados 75
Fig. 5.22 Diagrama de clases refinado auditar distrito..... 76
Fig. 5.23 Diagrama de secuencia auditar distrito 77
Fig. 5.24 Diagrama de clases refinado auditar voto 78
Fig. 5.25 Diagrama de secuencia auditar voto..... 79
Fig. 5.26 Diagrama de clases refinado inicia sistema..... 80
Fig. 5.27 Diagrama de secuencia inicia sistema 80
Fig. 6.1Modelo cliente/servidor SEVl 82
Fig. 6.2 Conexión entre los servidores y la terminal en SEVI 83
Fig. 6.3 Composición de los servidores que forman SEVI..... 84
Fig. 6.4 Diagrama de componentes Registro..... 86
Fig. 6.5 Página principal registro SEVI 86
Fig. 6.6 Página de registro SEVI 89
Fig. 6.7 Diagrama de componentes consulta estado del trámite..... 90
Fig. 6.8 Ventana de identificación para consultar el estado del trámite..... 91
Fig. 6.9 Página de aceptación de registro para el usuario. 91
Fig. 6.10 Diagrama de componentes votación..... 93
Fig. 6.11Boleta electoral SEVI..... 94
Fig. 6.12 Acuse de recibo para el Ciudadano SEVI 95
Fig. 6.13 Diagrama de componentes generación de resultados..... 96
Fig. 6.14 Consulta BDSC de las boletas electorales 96
Fig. 6.15 Consulta BDSC de los resultados al término de la jornada electoral 97
Fig. 6.16 Diagrama de componentes auditar distrito resultados votación..... 98
Fig. 6.17 Resultados generales de la jornada electoral SEVI 98
Fig. 6.18 Resultados del estado de Puebla de la jornada electoral SEVI 99

Fig. 6.20 Página de verificación del voto 100
Fig. 6.21 Acuse de recibo del votante 100
Fig. B.1 Archivo .bash_profile del usuario oracle..... 130
Fig. B.2 Vista del asistente para la manipulación de la base de datos..... 131

Agradecimientos

Agradezco al Consejo Nacional de Ciencias y Tecnología (CONACYT) y al Centro de Investigación y de Estudios Avanzados del IPN (CINVESTAV-IPN) por el apoyo económico ofrecido durante mis estudios.

De igual manera les reitero mi agradecimiento al Dr. Miguel Ángel León Chávez mi asesor y al Dr. Francisco Rodríguez Henríquez mi co-asesor, quienes con su experiencia, conocimientos y paciencia dirigieron mi proyecto de tesis.

Agradecimientos

Gracias a Dios por sus bondades, por este logro que es el intermedio para alcanzar una meta mayor.

Gracias a mi Padre y a mi Madre, su amor me hace fuerte y me impulsa a seguir adelante. Los Amo.

Gracias a mis compañeros y amigos de la maestría, de todos me llevo un grato recuerdo y una lección aprendida. ¡Éxito a todos!

Mi especial agradecimiento a Mara, Mónica, Víctor y Hugo con quienes conviví y forme una amistad más afectiva, a los tres los respeto y admiro, valoro sus consejos y sobretodo su confianza.

Para ti, que fuiste y eres mi apoyo incondicional en lo personal, familiar, profesional y espiritual.
Te quiero muchísimo mi gran amigo,

Alejandro Ramírez Sánchez.

Capítulo 1

Introducción

1.1 Descripción del problema

En México, los procesos electorales han evolucionado, prueba de ello es la reforma al Código Federal de Instituciones y Procedimientos Electorales (COFIPE), al adicionar en su libro sexto, los artículos 273 al 300, los cuales describen los pasos establecidos para la participación de los ciudadanos mexicanos radicados en el extranjero, para ejercer su derecho al voto, exclusivamente para la elección del Presidente de los Estados Unidos Mexicanos [1].

Esta reforma permite a los ciudadanos mexicanos radicados en el extranjero solicitar, registrar y emitir su voto a través del correo postal certificado.

El Instituto Federal Electoral (IFE), es el encargado de llevar a cabo este proceso con la ayuda del Servicio Postal Mexicano (SEPOMEX).

La estimación del número de mexicanos que habitan fuera de nuestro país y que cuentan con la credencial de elector, es aproximadamente de 4 millones de ciudadanos, sin embargo en el proceso electoral 2005-2006 en México, se recibieron poco más de 56 mil solicitudes de 86 países de los cinco continentes, de las cuales

cerca de 40 mil fueron aceptadas, teniendo como resultado la recepción de sólo 32,621 votos [2].

La modalidad del voto emitido por correo postal, tuvo una baja demanda por parte de los ciudadanos mexicanos radicados en el extranjero, una posible razón puede ser que era necesario conocer la dirección exacta del ciudadano y aunque la información era confidencial, debido a que la estancia de muchos de ellos no es legal dentro del país donde habitan, el temor de ser deportados provocó la negación de participar en este proceso.

Otro factor importante, fue el hecho de sostener el proceso teniendo como base los servicios de SEPOMEX, ya que esta institución no cuenta con los recursos necesarios para garantizar la secrecía y seguridad del voto por correo desde el exterior [3]. La mayoría de las solicitudes rechazadas fue por que no se enviaron por correo postal certificado.

En la actualidad, los medios electrónicos nos ofrecen una forma rápida y cómoda de manifestar el voto, a través de sistemas electrónicos de votación, los cuales usan boletas electrónicas, que permiten a los votantes emitir su voto y transmitirlo hacia la urna electoral también electrónica, donde será depositado y contabilizado al término de la jornada electoral por los funcionarios electorales.

Considerar el Internet para un sistema de votación se ha traducido en la posibilidad de fraude electoral debido a los ataques de seguridad de la propia red Internet, es por ello, que un sistema de votación ejecutado a través de Internet debe considerar a parte de las leyes electorales, cubrir los servicios de seguridad necesarios para cumplir con las características de un proceso electoral como son: la democracia y la transparencia, el anonimato del ciudadano y la integridad del voto [4].

Existen diferentes propuestas de sistemas de votación electrónica como por ejemplo el propuesto en Coahuila por parte del Instituto Electoral de Participación Ciudadana llamado Voto Extraterritorial [5]. Consiste en la automatización del proceso de votación por correo postal, sin embargo hace uso también del Servicio

Postal Mexicano, ya que basa su seguridad en una clave de identificación que es enviada al ciudadano por correo postal.

Un ejemplo más es el Sistema de Elecciones Electrónicas Seguras (SELES) [6], desarrollado en el Centro de Investigación y de Estudios Avanzados del IPN (CINVESTAV-IPN), ejecutado a través de Internet e implementa el protocolo de seguridad en votaciones electrónicas basado en Lin-Hwang-Chang [7] con la variación de utilizar firmas digitales DSA (Digital Signature Algorithm) en lugar de la firma digital ElGamal [8].

Este proyecto propone usar la red Internet para automatizar el proceso de votación de los mexicanos residentes en el extranjero, donde el ciudadano pueda registrar, solicitar y emitir su voto a través de Internet. El sistema propuesto se llama Sistema Electrónico de Votación por Internet (SEVI) y fue desarrollado usando la metodología del Proceso Unificado de Desarrollo de Software [9] y su Lenguaje Unificado de Modelado (UML) [10].

SEVI ofrece la ventaja a los ciudadanos mexicanos residentes en el extranjero de emitir su voto de una manera segura y sencilla, desde la comodidad de su casa u oficina, evitando el traslado a las oficinas de correo postal y el gasto en tiempo y economía que esto ocasiona.

Del lado del Instituto Federal Electoral, SEVI disminuiría los tiempos en los distintos periodos del proceso recibiendo solicitudes de los ciudadanos, verificándolas para rechazarlas o aceptarlas de forma automática; en la emisión del voto, recibir del ciudadano su voto en cuestión de segundos y en el conteo generar los resultados en el mismo día del proceso electoral dentro del país. De esta manera ya no es necesario esperar el tiempo que tarden en trasladarse por correo postal las solicitudes y las boletas electorales.

Sin embargo, dado que SEVI es un sistema ejecutado sobre Internet, lleva implícita la desconfianza sobre la transparencia del proceso y la seguridad del sistema.

Por lo anterior, para cubrir la seguridad se implementa la variación del protocolo basado en Lin-Hwang-Chang usado en SELES, del cual se desconoce vulnerabilidad en las fases que lo componen y

que son descritas en la sección 5.1.1. La razón por la cual no se considera a SELES en su totalidad es debido a que éste fue diseñado para un padrón electoral mediano de a lo más cinco mil votantes y el proceso electoral por correo postal en el año electoral 2005-2006 tuvo una demanda de poco mas de treinta mil votos emitidos.

SEVI consta de cuatro servidores expuestos en el modelo de diseño en el capítulo cinco, los cuales deben de estar físicamente separados y ejecutarse de manera independiente, sin embargo el sistema fue desarrollado cumpliendo sólo la última condición debido a que no se contó con la infraestructura suficiente como para implementarlo en cuatro máquinas servidores.

En las secciones siguientes se presentan el objetivo general, los objetivos específicos y la metodología seguida para el desarrollo de este proyecto.

1.2 Objetivo general

Desarrollar un sistema de software para automatizar el proceso de votación de los mexicanos radicados en el extranjero, para elegir al presidente de los Estados Unidos Mexicanos, como lo describe el libro sexto del COFIPE 2005, ejecutándolo a través de Internet.

1.2 Objetivos específicos

Construir con UML:

- Modelo de Casos de Uso: identificar los requisitos funcionales del sistema y modelarlos como casos de uso.
- Modelo de Análisis: se definirá el alcance del proyecto, además de identificar y acotar las tareas principales del sistema.

- Modelo de Diseño: se creará un diagrama de clases que permita la identificación de las clases principales que van a controlar el sistema y definir la iteración con las demás clases a fin de alcanzar el objetivo del sistema electrónico a través del diagrama de secuencia y de estados.
- Modelo de Implementación: iniciar la programación en un lenguaje que proporcione el mejor soporte para el sistema.
- Modelo de Pruebas: realizar pruebas parciales mientras se implementa el sistema y una prueba piloto para evaluar la funcionalidad del sistema.

Cubrir los requisitos funcionales:

- Registro del Ciudadano: que el ciudadano solicite su registro por Internet para votar en las elecciones presidenciales.
- Emisión del Voto: el ciudadano podrá emitir su voto por Internet a favor de su candidato predilecto.
- Generación de Resultados: el sistema debe ser capaz de realizar el conteo electrónicamente, entre o después de la votación.
- Auditoria: que los representantes de casilla, partido político o los integrantes de los consejos distritales puedan observar y evaluar el proceso electoral.
- Generación de Reportes: que el sistema permita generar reportes en las distintas etapas del proceso.

Cumplir:

- Las Leyes Electorales: el sistema debe operar de acuerdo a la ley electoral indicada en el libro sexto del COFIPE, artículos 273 al 300.
- Anonimato y no-Cohesión: garantizar que nadie sea capaz de determinar el valor del voto, ni vincularlo con el votante.

- Democracia: sólo pueden votar los ciudadanos registrados y por única ocasión.
- Transparencia: que sea posible auditar el proceso y que el proceso sea conocido y entendido por los votantes.
- Conveniencia: los votantes deben ser capaces de depositar su voto de manera rápida y con un mínimo de habilidad.
- Confiabilidad: el sistema debe ser robusto, sin pérdida de votos, sin fallas en el sistema, tanto en las máquinas servidores como en la comunicación a través de Internet.

Ofrecer los servicios de seguridad:

- Autenticación: sólo el votante autorizado puede emitir su voto.
- Confidencialidad: protección de la información en su transmisión a través de algoritmos de cifrado.
- Control de Acceso: evitar duplicidad en el registro y la votación.
- Integridad: la información y el voto del ciudadano no deben ser modificados, borrados o no detectados.
- No rechazo: controlar la información de entrada y salida, para evitar pérdidas y permitir o negar el servicio solicitado por el ciudadano.

1.3 Metodología

La construcción de software requiere que la comunidad de desarrolladores trabaje de forma coordinada en un proceso que integre las múltiples facetas del desarrollo, que proporcione una guía para ordenar las actividades del equipo, dirija las tareas de cada desarrollador por separado y del equipo como un todo, que especifique

los artefactos que deben desarrollarse y ofrezca los criterios para el control y la medición de los productos y actividades del proyecto.

El Proceso Unificado de Desarrollo de Software (PUDS) [9] es un marco genérico que puede especializarse para una gran variedad de sistemas, en diferentes áreas de aplicación, organizaciones, niveles de aptitud y tamaños de proyecto. Los aspectos verdaderos del Proceso Unificado de desarrollo de software se resumen en tres frases clave: Dirigido por Casos de Uso, centrado en la arquitectura, e iterativo e incremental.

- Dirigido por casos de Uso:

  Un sistema de software ofrece servicios a sus usuarios, el término usuario no sólo se refiere a usuarios humanos, sino también a otros sistemas.

  Un caso de uso es un fragmento funcional del sistema que proporciona al usuario un resultado importante. Los casos de uso representan requisitos funcionales y todos los casos de uso forman un modelo de casos de uso.

  Una especificación funcional debe responder la pregunta ¿Qué debe hacer el sistema para cada usuario? Aunque es cierto que los casos de uso guían el proceso, no se desarrollan aisladamente, se desarrollan a la vez que la arquitectura del sistema. Por tanto la arquitectura del sistema como los casos de uso maduran según avanza el ciclo de desarrollo.

- Centrado en la Arquitectura:

  El concepto de arquitectura incluye los aspectos estáticos y dinámicos del sistema. La arquitectura surge de las necesidades de la empresa.

  Cada producto tiene tanto una función como una forma, la función corresponde a los casos de uso y la forma a la arquitectura. Para encontrar esa forma el arquitecto usa sólo

los casos de uso clave, que corresponden al 10 o 5 por ciento de todos los casos de uso.

- Iterativo e incremental:

  Es práctico dividir el trabajo en partes más pequeñas o mini proyectos. Cada mini proyecto es una iteración. Las iteraciones se seleccionan y se ejecutan de forma planificada.

El Proceso Unificado de Desarrollo de Software utiliza el Lenguaje Unificado de Modelado (Unified Modeling Language, UML) [10] para preparar todos los esquemas de un sistema de software.

UML es un lenguaje visual del modelado y el modelado es una parte central de todas las actividades que conducen a la producción del buen software. Los modelos que se construyen son para comunicar la estructura deseada y el comportamiento del sistema, para visualizar y controlar la arquitectura del sistema, para comprender mejor el sistema que se está construyendo y para controlar el riesgo.

Por tanto es apropiado para modelar desde sistemas de información en empresas hasta aplicaciones distribuidas basadas en la Web.

Este proyecto de tesis usa el Proceso Unificado de Desarrollo de Software para el desarrollo del sistema propuesto SEVI, construyendo los modelos de casos de uso, análisis, diseño, implementación y pruebas con UML.

De las tres clases de construcción de UML, se tomaron de cada una de ellas lo siguiente:

- *Elementos*: casos de uso, clases activas, componentes, nodos, mensajes, paquetes y notas.
- *Relaciones*: dependencias, asociaciones y realizaciones.
- *Diagramas*:
  - Diagrama de Casos de Uso: Muestra un conjunto de casos de uso y sus actores, es especialmente

importante en el modelado y organización del comportamiento de un sistema.

- Diagrama de Clases: Modelado de sistemas orientados a objetos y muestra un conjunto de clases, interfaces y colaboraciones, así como sus relaciones.
- Diagrama de Secuencia: Consta de un conjunto de objetos y sus relaciones, incluyendo los mensajes que pueden ser enviados entre ellos. Este tipo de diagramas resalta la ordenación temporal de los mensajes.
- Diagrama de Componentes: diagrama que cubre la vista de implementación del sistema, se relaciona con los diagramas de clases en que un componente corresponde con una o más clases, interfaces o colaboraciones.
- Diagrama de Despliegue: Muestra la configuración de nodos de procesamiento en tiempo de ejecución y los componentes que residen en ellos.

1.4 Estructura del documento

El resto del trabajo está estructurado como sigue:

En el capítulo 2, se presenta el estado del arte, donde se mencionan los distintos tipos de sistemas de votación y se enfatiza en el Sistema de Elecciones Electrónicas Seguras, describiendo brevemente el protocolo de seguridad que utiliza.

En el capítulo 3, se hace un análisis a detalle del proceso electoral por correo postal para la votación presidencial de los ciudadanos mexicanos en el extranjero.

En el capítulo 4, se propone para la automatización de la votación por correo postal el Sistema Electrónico de Votación por

Internet (SEVI), construyendo los modelos de casos de uso y análisis con UML.

En el capítulo 5, se aborda la seguridad del sistema y se construye el modelo de diseño con UML, presentando los diagramas de clase y secuencia.

En el capítulo 6, se describe el modelo de implementación, con los diagramas de componentes y despliegue de UML, se muestra la interfaz del sistema con sus usuarios y termina con la descripción de una prueba inicial para comprobar la funcionalidad del sistema.

En el capítulo 7, se presentan las conclusiones de este trabajo y se exponen los trabajos futuros.

En la parte final del documento se exponen dos apéndices. El apéndice A muestra el Libro Sexto del COFIPE que fue decretado el 30 de Junio de 2005 y en el cual nos basamos para el desarrollo del sistema SEVI. El apéndice B es una ayuda a la instalación de los paquetes de software que utiliza el sistema SEVI.

Capítulo 2

Sistemas de Votación

2.1 Sistema de votación convencional

Las elecciones dignas de confianza son esenciales para la democracia, la realización de ellas requiere un equilibrio entre seguridad, costo y conveniencia. En un sistema de votación convencional, los votantes pueden confiar en algunos aspectos del proceso, en base a sus propias acciones y observaciones. Existe un registro de su voto al marcar de manera manual la boleta electoral impresa en papel y aunque su participación termina al ingresar la boleta en la urna electoral, debido a que se utiliza papelería electoral, los votantes tienen plena conciencia de que cada paso que realizan es supervisado por los funcionarios electorales y los representantes de cada partido político o coalición, saben que existe un registro de su voto, que puede ser verificado y no destruido o alterado sin que haya una evidencia.

En contra parte a esa seguridad en la comprobación del proceso, la lentitud de este, es lo que más afecta en el desarrollo de las elecciones. El traslado de los ciudadanos a las casillas electorales, la cola de espera para la emisión del voto, la tardanza en el conteo y el dictamen del ganador son las razones más sobresalientes para buscar

la automatización del proceso. Usando la tecnología y los servicios que nos ofrecen los medios electrónicos, los procesos de votación pueden realizarse en periodos de tiempo más cortos y lograr mejor precisión en los resultados.

2.2 Sistemas de votación electrónica

Los sistemas de votación que no producen un registro físico o en papel, como lo son los sistemas electrónicos, deben contar con un plus adicional de confianza en los elementos que lo componen, como pueden ser monitores touch screen [11], tarjetas, máquinas, etc., debido a que se pierde la transparencia y la comprobación de los resultados.

Algunos de los sistemas electrónicos de votación son los siguientes:

Los sistemas “punch-card” [12,13], donde los votantes usan tarjetas electrónicas, que deben marcar con su voto e ingresarla a un tabulador centralizado, para que éste capture el voto y posteriormente se realice el conteo; los errores que pueden ocurrir, es que el votante se confunda al momento de marcar la tarjeta electrónica, que el tabulador no funcione correctamente o que se pierda o dañe la tarjeta electrónica.

Los sistemas que usan dispositivos de lectura óptica, el votante marca su voto en la boleta electoral, llenando un circulo, cuadrado o rectángulo, para que después sea leída por un scanner el cual registra el voto y realiza el conteo automáticamente.

Los sistemas que manejan máquinas electrónicas de registro o grabación [14,15,16] (direct-recording electronic machines, DRE’s) como por ejemplo: las máquinas “touch-screen” que permiten a los votantes emitir y transmitir el voto tocando una opción en la boleta electrónica que se muestra en la pantalla LCD; las máquinas “punch-key” usan un teclado para hacer la selección en la boleta electrónica y

las máquinas “wheel” requieren que el votante rote una rueda y presione un botón.

Las máquinas especiales que utilizan los sistemas electrónicos mencionados, deben cubrir plenamente la confianza de los funcionarios electorales, respecto a su fabricación, mantenimiento y funcionamiento ya que son la base principal del proceso electoral [17].

En la votación electrónica, se aumenta el potencial para el fraude a grande escala, si muchas máquinas de votación funcionan con el mismo software y no existe ningún mecanismo para que los votantes verifiquen que sus votos estén registrados correctamente o para que los funcionarios electorales puedan realizar un recuento significativo, un defecto intencional o accidental sobre el software puede afectar irrevocablemente el resultado de la elección [18].

Un sistema de votación electrónica debe producir constantemente expedientes que proporcionen los medios por los cuales pueda realizarse un conteo o reconteo exacto, asegurando así la confiabilidad, la seguridad y la comprobabilidad de la elección y que esto pueda traducirse en una democracia estable. La conveniencia y la comodidad del votante y la rapidez del proceso no son ningún sustituto para la exactitud de los resultados y la confianza en el proceso electoral [19].

2.3 Sistemas de votación electrónica por Internet

En un sistema de votación electrónica por Internet, la máquina de votación puede ser cualquier computadora personal (PC) conectada a Internet. El proceso que sigue el votante es solicitar la boleta electoral electrónica, marcar su voto y transmitirla por Internet hacia la urna electoral donde el voto será depositado y contabilizado al término de la jornada electoral. Sin embargo, recurrir al uso del Internet para un

sistema de votación, trae consigo exponerse a los ataques provenientes de la propia red Internet [20].

Dado que la máquina de votación estará conectada a Internet, está expuesta a ser infectada por virus, gusano o spam degradando la funcionalidad del sistema de elección o alterando el valor del voto; incluso podría ubicarse en un lugar donde no existan las condiciones para emitir libremente ni de manera secreta el voto y por último, podría ser monitoreada por el administrador de la red y observar el voto antes de ser cifrado y transmitido.

Por otro lado, la red Internet es usualmente un canal de comunicación inseguro, por lo que el sistema de votación debe proveer los servicios de seguridad para evitar que el voto sufra ataques pasivos y activos (interceptado, modificado, borrado o fabricado).

El poner en marcha una elección pública engloba la creación de leyes electorales que dejen en claro el funcionamiento del sistema de software y los procedimientos a seguir en caso de cualquier contingencia.

El sistema de votación electrónica debe cubrir los requisitos funcionales en el proceso de votación, así como los servicios de seguridad necesarios para protegerse de los posibles ataques provenientes de la red.

En general, un sistema de votación electrónico debe cubrir los siguientes criterios [21]:

1. *Autenticación*: sólo el votante autorizado puede emitir su voto.
2. *Unicidad*: ningún votante debe votar más de una vez.
3. *Exactitud*: el sistema debe registrar y procesar los votos correctamente.
4. Integridad: los votos no deben de ser modificados, olvidados, borrados o no detectados.

5. *Verificación y Auditoria*: debe ser posible verificar que los votos se hayan contado correctamente al final de la elección y demostrar así la autenticidad de la misma.
6. *Confiabilidad*: el sistema debe ser robusto, sin perdida de votos, sin fallas en el sistema, tanto en las máquinas PC, los servidores como en la comunicación a través de Internet.
7. *Anonimato y no Cohesión*: nadie debe ser capaz de determinar el valor del voto ni vincularlo con el votante.
8. *Flexibilidad*: tener una variedad de formatos para las boletas de votación a fin de hacerlos compatibles con la variedad de plataformas y tecnologías.
9. *Conveniencia*: los votantes deben de ser capaces de depositar su voto de manera rápida y con un mínimo de habilidad.
10. *Certificación*: el sistema electoral debe ser estable, para una elección oficial debe de contar con los criterios necesarios para su validez.
11. *Transparencia*: los votantes deben de entender y conocer el proceso de votación.
12. *Costo-Eficiencia*: el sistema de votación debe ser accesible y eficiente.

Como ejemplo de algunos sistemas desarrollados y utilizados para la votación electrónica se encuentran, el sistema SERVE (Secure Electronic Registration and Voting Experiment) [22], implementado en las votaciones primarias y secundarias del 2004 en Estados Unidos de Norteamérica, el cual está basado en la Web, los votantes hacían un registro previo y posteriormente votaban al conectarse al servidor desde cualquier computadora conectada a Internet.

En México, el sistema Voto Extraterritorial [5] fue desarrollado en el Instituto Electoral y de Participación Ciudadana del estado de Coahuila para las elecciones presidenciales de 2006, el cual usa un código secreto, si es válido permite la votación a través de cualquier

computadora, requiere de un registro previo y el envío por correo del código secreto.

Un último ejemplo es SELES (Sistema de Elecciones Electrónicas Seguras) [6], desarrollado en el CINVESTAV-IPN. SELES es un sistema que puede ser ejecutado desde dispositivos móviles conectados a Internet, utiliza la arquitectura cliente/servidor y cubre los servicios de seguridad implementando la versión mejorada del protocolo de seguridad de Lin-Hwang-Chang [8]. Está diseñado para un padrón electoral mediano de a lo más cinco mil votantes y requiere de un registro previo.

El protocolo de seguridad Lin-Hwang-Chang [7] usa firmas a ciegas, firmas digitales ElGamal, detecta al votante que intenta emitir su voto más de una vez (votante tramposo) e incrementa la protección a un posible fraude. Consta de tres fases: Autenticación, Votación y Conteo. Para su implementación en SELES, este protocolo fue modificado, sustituyendo a la firma digital ElGamal por la firma digital DSA (Digital Signature Algorithm), la justificación principal fue el hecho de que ElGamal utiliza aritmética modular *mod p y mod (p-1)*, mientras que DSA usa aritmética modular *mod p* y *mod q*.

Los votantes necesitan previamente obtener su Certificado Digital a través de un registro, así como un par de llaves pública y privada para la protección de su voto, esto es requisito fundamental para que puedan emitir su voto.

El protocolo usa un servidor en cada una de sus fases, el Servidor de Autenticación (SA) en la fase de autenticación, el Servidor de Votación (SV) en la fase de votación y el Servidor de Conteo (SC) en la fase de conteo.

Los pasos que sigue el protocolo en cada una de sus fases son los siguientes:

a. Fase de Autenticación
    i. El votante solicita las firmas a ciegas al SA, agregando en la solicitud su firma y certificado digital.
    ii. El SA autentica al votante con la firma y el certificado digital, si es válido entonces le genera un identificador único, lo almacena para su control en la base de datos del SA, firma a ciegas el mensaje, lo cifra con la llave pública del votante y se lo envía.
    iii. El votante recibe el mensaje, lo descifra con su llave privada para obtener su identificador único y el mensaje firmado por SA.
b. Fase de Votación
    i. El votante emite su voto y lo firma usando la firma digital DSA. Por último envía el boleto de votación con la firma del SA y la firma del voto al SV.
    ii. El SV recibe el boleto de votación y verifica que las firmas recibidas sean correctas, si es así entonces lo almacena en su base de datos y envía al ciudadano un acuse de recibido.
c. Fase de Conteo
    i. Al término de la jornada electoral, el SV envía los boletos de votación válidos al SC.
    ii. El SC recibe los boletos de votación y envía al SV un acuse de recibido.
    iii. El SC cuenta por una sola ocasión los votos y verifica que no sean duplicados.
    iv. Si encuentra un boleto duplicado, solicita al SA la identidad del votante tramposo.

Haciendo un resumen de la seguridad implementada en SELES, el protocolo de seguridad basado en Lin-Hwang-Chang con la sustitución de ElGamal por DSA, usa tres servidores que trabajan de manera independiente, que permiten al ciudadano ser anónimo al valor de su voto y a pesar de eso poder ser identificable si incurre en el acto de votar en más de una ocasión. El votante puede auditar su voto, usando el acuse de recibo entregado por el servidor de votación, al verificar las listas de los resultados y de los acuses de recibo entregados a cada votante.

Capítulo 3

Voto por Correo Postal en México

3.1 Reforma electoral 2005

La reforma electoral de 1996 representó un hito en la historia política de México porque en definitiva permitió la alternancia pacífica en la titularidad del Poder Ejecutivo Federal en el año 2000. Sin embargo, aún quedaba pendiente cumplir con uno de los fundamentos que motivaron la realización de esta reforma y era el de diseñar un mecanismo que permitiera el ejercicio efectivo de los derechos políticos de los ciudadanos mexicanos residentes en el extranjero.

El 22 de febrero de 2005, la Cámara de Diputados aprobó una reforma a la ley electoral que permitiría a los mexicanos residentes en el extranjero, mayoritariamente en EEUU, votar en las elecciones a partir de 2006. El proyecto de ley fue enviado al Senado para su análisis, discusión y aprobación, con el fin de convertirse en ley.

El 27 de abril de 2005, el Senado de la República aprobó una minuta para que en tales elecciones participaran los mexicanos radicados en el extranjero, con la emisión de su voto a través del correo postal [23].

Los consejeros del Instituto Federal Electoral (IFE), responsables de la organización de las elecciones, reiteraron su rechazo a votaciones directas en el extranjero, semejante a las que se realizan en México e insistieron en que el voto postal era “técnicamente viable”.

3.2 Voto por correo postal

Los pasos que debe seguir el procedimiento por correo postal certificado según el Código Federal de Instituciones y Procedimientos Electorales (COFIPE) [1], en su libro sexto, artículos del 273 al 300 se presentan a continuación:

Todo ciudadano mexicano que resida en el extranjero, podrá ejercer su derecho al voto, exclusivamente para la elección de Presidente de los Estados Unidos Mexicanos. Artículo 273.

El ciudadano solicitará su participación en el proceso, por escrito, con su firma autógrafa o en su defecto con su huella digital, llenando una solicitud de inscripción. Artículo 274.

La solicitud de inscripción, deberá ser enviada entre el 1o. de octubre del año previo, y hasta el 15 de enero del año de la elección presidencial, por los ciudadanos a la Dirección del Registro Federal de Electores, por correo postal certificado junto con la copia fotostática legible de su credencial de elector (anverso y reverso) y un documento que conste el domicilio que manifiesta tener. Para la verificación de los periodos de recepción, se tomará en cuenta la fecha estampada en el sobre de envío y no se aceptarán las solicitudes que lleguen después del 15 de febrero del año electoral. El ciudadano podrá consultar al

Instituto vía electrónica o telefónica, el estado de su inscripción. Artículo 275.

La solicitud de inscripción contendrá una leyenda que el ciudadano debe aceptar para continuar con su trámite, donde autoriza al IFE darlo de baja temporalmente de la Lista Nominal de Electores (LNE) e ingresarlo a la Lista Nominal de Electores en el Extranjero (LNEE), solicita el envío de la boleta electoral a su domicilio en el extranjero y una vez terminado el proceso electoral reinscribirse en la LNE en la sección correspondiente a la indicada en su credencial de elector. Artículo 276.

La Lista Nominal de Electores en el Extranjero (LNEE) es de carácter temporal y sólo para los efectos del proceso electoral por correo postal, se formará de los nombres de ciudadanos que se encuentren en el Padrón Nacional con credencial de elector, que viven en el extranjero y solicitan su inscripción en dicha lista, no contendrá la fotografía del ciudadano y estará sujeta a verificación para garantizar su veracidad. Artículo 277.

El formato de la solicitud de inscripción estará disponible, del 1ro de octubre del año anterior a la elección hasta el 15 de enero del año electoral, por Internet y en las Sedes Diplomáticas de México en el extranjero. Artículo 278.

La Dirección Ejecutiva del Registro Federal de Electores, recibirá y atenderá las solicitudes conforme su fecha de recepción. Una vez verificado el cumplimiento de los requisitos, realizará la baja temporal del ciudadano en la LNE y su ingreso a la LNEE, conservando los documentos enviados hasta concluir el proceso electoral. Artículo 279.

Una vez terminado el periodo de recepción la Dirección Ejecutiva procederá a elaborar las listas nominales de electores en el extranjero, de acuerdo al domicilio en el extranjero, con el fin de enviar las boletas electorales a los ciudadanos. Elaborará además otra lista ordenada por entidad federativa y distrito electoral, para efectos de escrutinio y votación. La información contenida en estas listas debe ser de carácter

confidencial para el personal del Instituto y los representantes de partidos políticos que las verifican. Artículo 280.

Los representantes de cada partido político en la Comisión Nacional de Vigilancia, tendrán derecho a la verificación de la LNEE, a través de los medios electrónicos con que cuente la Dirección Ejecutiva de Registro Federal de Electores. Artículo 281.

A más tardar el 15 de marzo del año electoral, la Dirección Ejecutiva entregará a los partidos políticos las LNEE, quienes podrán formular observaciones hasta el 31 de marzo. En caso de modificaciones, tendrán hasta el 15 de mayo para informar a la Comisión Nacional de Vigilancia y al Consejo General, para las impugnaciones, se llevarán ante el Tribunal Electoral. Si no se presentan modificaciones o impugnaciones el Consejo General declarará la LNEE como válida. Artículo 282.

La Junta Federal Ejecutiva deberá ordenar la impresión de las boletas electorales que llevarán la leyenda de “Mexicano residente en el extranjero”. El número de boletas impresas será igual al número de electores en la LNEE. Artículo 283.

La boleta electoral, la documentación y demás material necesario para el ejercicio del voto, deberá estar lista a mas tardar el 15 de abril del año electoral, para ser enviada a cada ciudadano por correo certificado con acuse de recibo, envío que concluirá el 20 de mayo del año de la elección. Artículo 284.

El ciudadano deberá ejercer su derecho al voto, de manera secreta, libre y directa, marcando el recuadro que corresponda a su preferencia, al recibir la boleta electoral y siguiendo los pasos del instructivo anexo. Artículo 285.

Hecha su elección, el ciudadano deberá doblar e introducir la boleta electoral en el sobre marcado con su clave de elector, sellándolo de forma que asegure el secreto del voto y enviarlo por correo certificado, al Instituto Federal Electoral. Artículo 286.

La Junta General Ejecutiva dispondrá lo necesario para recibir y registrar los sobres, señalando el día y clasificándolos conforme a las listas nominales de electores para efecto de escrutinio y cómputo. Colocarán la leyenda “voto” a lado del nombre del elector en la LNEE y se resguardarán los sobres recibidos y el secreto del voto. Artículo 287.

Serán considerados como votos emitidos en el extranjero los que se reciban veinticuatro horas antes del inicio de la jornada electoral. Para los que se reciban después, se elaborará una relación, acto seguido y sin abrir el sobre, en presencia de los representantes de partidos políticos se procederá a su destrucción. Artículo 288.

Con base en la LNEE, el Consejo General determinará el número de mesas de escrutinio y cómputo que correspondan a cada distrito electoral. Cada mesa de escrutinio contará con un presidente, un secretario, dos escrutadores y un representante de cada partido político, y permitirá hasta 1500 votos. Artículo 289.

Las mesas de escrutinio se instalarán a las 17 horas del día de la jornada electoral. A las 18 horas se iniciará el escrutinio y cómputo de la votación emitida en el extranjero. Artículo 290.

El presidente de cada mesa de escrutinio, sumará los electores marcados con la palabra “voto”, resultado que se comparará con la suma hecha por los escrutadores de los sobres que contienen las boletas electorales. Si son iguales, el presidente extraerá la boleta electoral doblada del sobre y la colocará en la urna electoral. Si no llegara a encontrarse o se encontraran más de dos boletas, los votos se considerarán como nulos. Una vez terminado lo anterior, dará inicio el escrutinio y cómputo. Artículo 291

Las actas de escrutinio y cómputo de cada mesa serán agrupadas conforme al distrito electoral que corresponda. El personal del Instituto designado por la Junta General Ejecutiva, procederá, en presencia de los representantes generales de los partidos políticos, a realizar la suma de los resultados consignados en las actas para obtener el resultado de la votación emitida en el extranjero para la

elección de Presidente de los Estados Unidos Mexicanos por distrito electoral, que será asentado en el acta de cómputo correspondiente a cada distrito electoral. Artículo 292.

Al concluir totalmente el escrutinio, el Secretario General, dará a conocer al Consejo General los resultados por partido de la votación emitida en el extranjero para Presidente de los Estados Unidos Mexicanos. Artículo 293.

La Junta General Ejecutiva, antes del miércoles siguiente al día de la jornada electoral, entregará a cada uno de los Consejos Distritales, copia del acta de cómputo distrital, con copia a todos los partidos políticos. Artículo 294.

En cada uno de los Consejos Distritales el presidente del mismo informará a sus integrantes el resultado consignado en la copia del acta distrital para que sean sumados a los obtenidos del cómputo de los resultados de las casillas instaladas en el respectivo distrito. Artículo 295.

Los partidos políticos nacionales y sus candidatos no podrán realizar campañas electorales en el extranjero. Artículo 296.

La violación al artículo anterior podrá ser denunciada ante el Secretario Ejecutivo del Instituto, por los representantes de cada partido político. Artículo 297.

Para el cumplimiento de las atribuciones y tareas que otorga el Libro Sexto al Instituto Federal Electoral, la Junta General Ejecutiva propondrá al Consejo General, en el año anterior al de la elección presidencial, la creación de las unidades administrativas que se requieran. Artículo 298.

El costo de los servicios postales derivado de los envíos que por correo realice el Instituto a los ciudadanos residentes en el extranjero, será previsto en el presupuesto del propio Instituto. Artículo 299.

El Consejo General proveerá lo conducente para la adecuada aplicación de las normas contenidas en el Libro Sexto. Artículo 300.

La Fig. 3.1 ilustra el procedimiento de la votación de los mexicanos residentes en el extranjero por correo postal, según los artículos 274-293, descritos anteriormente.

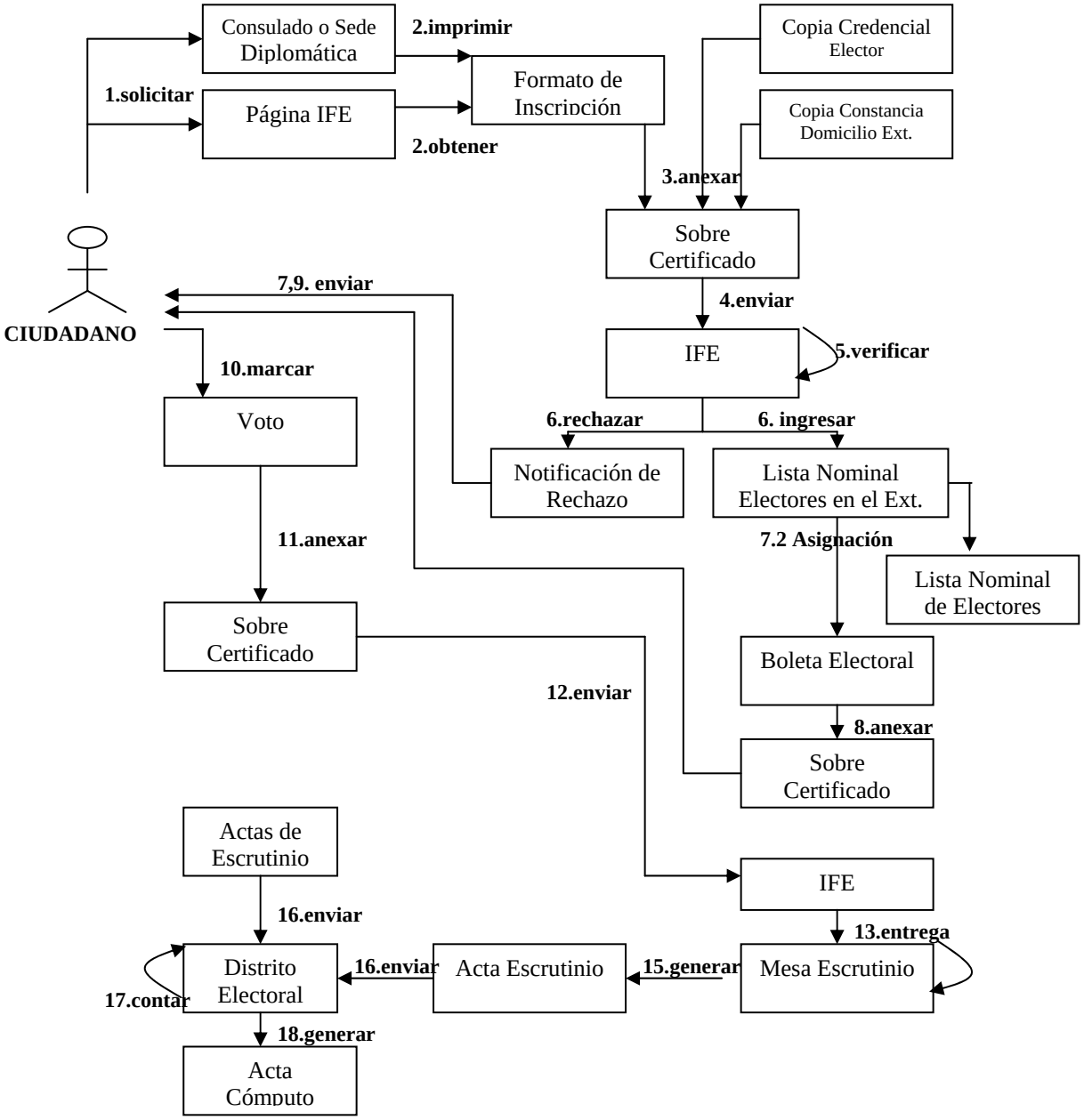


Fig. 3.1 Procedimiento de votación en el extranjero, modalidad por correo postal certificado.

Dado que el objetivo principal de este proyecto de tesis es la automatización del proceso electoral descrito anteriormente, en el próximo capítulo, se identifican los casos de uso y se hace un análisis general del sistema.

Capítulo 4

Sistema Electrónico de Votación por Internet (SEVI)

En este capítulo se presentan los modelos de casos de uso y de análisis utilizando UML. El modelo de casos de uso captura los requerimientos del usuario. El modelo de análisis especifica los requerimientos del usuario. La especificación puede ser informal, semiformal o formal (usando métodos formales de especificación, tales como máquinas de estados finitos, redes de Petri, SDL, etc.)

4.1 Modelo de casos de uso

El Sistema Electrónico de Votación por Internet (SEVI), es una propuesta para la automatización del proceso electoral por correo postal certificado en México, su operación debe cumplir con los pasos de la ley electoral descritos en el capítulo anterior.

Haciendo un resumen de las normas expuestas en cada artículo del Libro Sexto del COFIPE, para que un ciudadano mexicano radicado en el extranjero pueda votar, debe solicitar su registro a la LNEE, enviando al IFE su solicitud de inscripción, consultar el estado de su

trámite (si lo desea), recibir la boleta electoral, marcar su voto, asegurar la boleta electoral y por último enviarla al IFE. Del lado del Instituto Federal Electoral (IFE), primero: debe publicar, recibir y autorizar las solicitudes de los ciudadanos; segundo: mostrar a los representantes de los partidos políticos la lista nominal generada para efecto de verificación y modificación; tercero: enviar, recibir y contar boletas electorales; cuarto: sumar los votos de cada boleta electoral válida y obtener el resultado de la votación por mesa de escrutinio; quinto: obtener los resultados de la votación por distrito electoral y sexto: informar a los consejeros electorales y a los partidos políticos el resultado de la votación.

De lo anterior podemos mencionar al menos cuatro fases (registro, votación, conteo e información o auditoria), para abarcar el proceso de votación por correo postal certificado. Dado que la implementación del sistema es sobre la arquitectura cliente/servidor y por medio de Internet, un primer esquema de funcionalidad de SEVI se ilustra en la Figura 4.1.

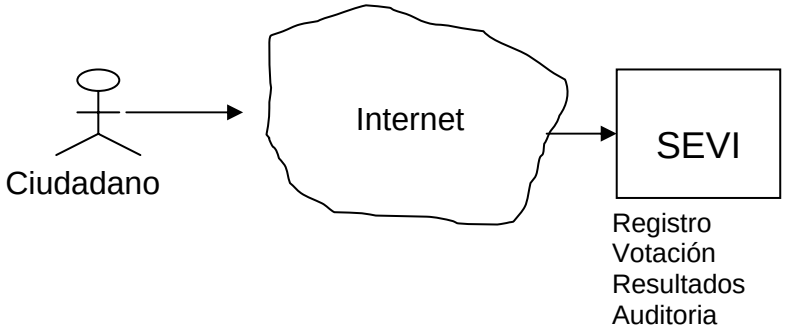


Fig. 4.1 Primera aproximación de funcionalidad de SEVI

El papel de SEVI será el desempeñado por el IFE de tal forma que cada fase cumpla con las normas establecidas en los artículos, sin embargo cada artículo requiere de un ajuste a fin de poder ser implementado en SEVI, con la condición de no alterar las disposiciones o normas de la ley electoral. La tabla 4.1 nos muestra los artículos, las

normas establecidas en cada uno de ellos, la fase en la que pueden ser implementados y cómo pueden ser implementados en SEVI.

Art.	Norma	Fase	Implementación
273	Derecho al voto	Registro	Publicar vía Internet el formato de registro
274	Solicitud de Inscripción	Registro	Formato de registro electrónico
275	Envío de la solicitud por parte del ciudadano al IFE y consulta del estado del trámite a través de Internet o vía telefónica.	Registro / Consulta	Enviar a través de Internet el formato electrónico/ consultar el estado del trámite
276	Autorización del ciudadano para la manipulación de sus datos al IFE	Registro	Aceptación del ciudadano a los términos y disposicio-nes de seguridad y manejo de su información.
277	Formato de la Lista Nominal Electoral en el Extranjero (LNEE)	Registro	Creación de la base de datos (BDR) donde se almacenará la LNEE
278	Periodo abierto para la solicitud de inscripción	Registro	Servidor Web disponible para publicar y recibir solicitudes de registro
279	Verificación de la solicitud. Aceptación: baja temporal del ciudadano en la LNE e ingreso en la LNEE	Registro	Consulta y baja temporal del registro del ciudadano en la LNE y alta del mismo registro en la LNEE
280	Elaboración de la LNEE	Auditoria	Generación de reportes de la LNEE, para efecto de auditoria.
281	Verificación de la LNEE por los partidos políticos	Auditoria	Entregar al personal autorizado, bajo previa identificación reportes de la LNEE vía Internet.

282	Impugnación a la LNEE por los partidos políticos	Auditoria	Modificación de la LNEE, bajo previa autorización
283	Impresión de las boletas electorales	Votación	Generación de la Boleta Electoral Electrónica (BEE), previa identificación del ciudadano y creación de la base de datos (BDA) para almacenar al ciudadano identificado (Autenticado)
284	Periodo de envío de las boletas electorales al ciudadano	Votación	Servidor Web disponible para identificación del ciudadano y presentación de la BEE en el navegador
285	Emisión del voto	Votación	Selección en la BEE del valor del voto
286	Seguridad de la boleta electoral	Votación	Protección del voto por medio del protocolo de seguridad
287	Recepción de las boletas electorales	Votación	Creación de la base de datos (BDV) para el almacenamiento de la BEE, después de ser verificadas y aceptadas como válidas
288	Periodo de recepción de las boletas electorales	Votación	Servidor Web disponible para la recepción de las BEE
289	Determinación del número de mesas de escrutinio	---	Los 300 distritos electorales existentes están disponibles en SEVI
290	Instalación de las mesas de escrutinio	Conteo	Servidor Web disponible para la recepción de las BEE válidas
291	Inicio del escrutinio	Conteo	Creación de la base de datos (BDC) para el almacenamiento de las BEE válidas.

292	Generación del acta de escrutinio por distrito electoral	Conteo	Suma por distrito electoral de los votos emitidos por partido electoral y almacenamiento del resultado en la BDC
293	Reporte de resultados de la votación	Auditoria	Consulta de la BDC del resultado por distrito electoral
294	Entrega de la copia del acta de cómputo distrital a consejeros distritales y a partidos políticos	Auditoria	Entregar al personal autorizado, bajo previa identificación reportes de la votación.
295	Suma de los votos emitidos en el extranjero con los emitidos en territorio nacional por distrito electoral.	---	No es posible realizarla desde SEVI, la suma se hace desde cada distrito electoral
296	Inválidas las campañas electorales fuera del país	---	Es una disposición legal, independiente del funcionamiento de SEVI
297	Denuncia a la violación del artículo 296	---	Es una disposición legal, independiente del funcionamiento de SEVI
298	Creación de unidades administrativas requeridas	---	Es una disposición legal, independiente del funcionamiento de SEVI
299	Costos de inversión	---	Es una disposición legal, independiente del funcionamiento de SEVI
300	El Consejo General proveerá lo adecuado para la aplicación de estas normas.	---	Es una disposición legal, independiente del funcionamiento de SEVI

Tabla 4.1 Artículos automatizados y no automatizados en SEVI del libro sexto del COFIPE.

El artículo 275 menciona una consulta por parte del ciudadano al IFE respecto al estado de su trámite por vía telefónica o por Internet. La consulta es opcional, es decir, el que la solicite o no el ciudadano no afecta el proceso electoral ya que sólo es meramente informativa. No obstante, debido a que es necesario proveer al ciudadano de un certificado digital y de un par de llaves de seguridad (pública y privada), para seguridad del proceso que será implementado en Internet, la consulta se vuelve obligatoria, con el fin de que el ciudadano obtenga esta información necesaria para emitir su voto.

Un servicio que no provee el proceso electoral analizado, es el hecho de permitirle al ciudadano verificar o auditar que su voto fue efectivamente contabilizado después de haberlo emitido. En SEVI, se considera en el análisis ofrecer este servicio.

Hasta ahora hemos hablado sólo de los ciudadanos, sin embargo también forman parte del proceso electoral las personas que lo vigilan, como lo son: los partidos políticos a través de sus representantes, los consejeros electorales, los integrantes del Consejo General, etc. a todas estas personas en este proyecto les llamaremos Representantes.

Los Representantes podrán solicitar reportes a SEVI en las distintas fases del proceso como es la verificación de la LNEE y la generación de los resultados. Para controlar la generación de los reportes, a los Representantes se les asignarán claves de identificación (login y password), mismas que serán usadas para que se autentiquen ante SEVI.

Los administradores del sistema son parte fundamental en la implementación de SEVI, este grupo de personas les llamaremos Administradores, los cuales se encargarán de inicializar y dar mantenimiento al sistema, de la consulta y actualización previa autorización de las bases de datos, el alta de los Representantes en el sistema, etc.

Hablando en término de servicios, los que puede ofrecer SEVI hasta ahora identificados para el ciudadano son: el registro, la consulta

del estado del trámite, la emisión de su voto y la auditoria del mismo; para el Representante son: la auditoria de la LNEE y de los resultados de la votación; para los Administradores son: la administración general del sistema y su inicialización.

La Figura 4.2 nos muestra los servicios ofrecidos a través de los casos de uso y los actores a quienes sirven.

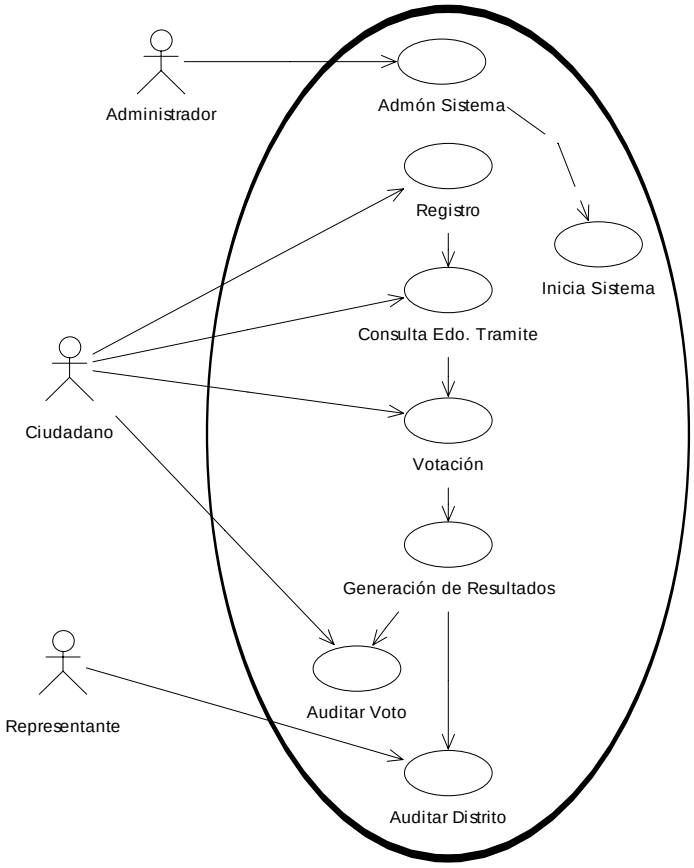


Fig. 4.2 Diagrama de casos de uso de SEVI.

4.2 Modelo de análisis

En esta sección se detallarán las funciones para cada caso de uso ilustrado en el diagrama de casos de uso.

4.2.1 Caso de uso registro

Este caso de uso tiene como actor al Ciudadano quien representa al ciudadano mexicano radicado en el extranjero, el cual solicita el servicio de registro a la Lista Nominal de Electores en el Extranjero (LNEE).

Las funciones de este caso de uso son las siguientes:

- Proporcionar al Ciudadano, una forma electrónica identificada como Solicitud de Registro, a partir del 1ro de octubre del año previo al de la elección hasta el 15 de enero del año electoral. Artículo 278.
- Recibir la forma electrónica, llenada por el Ciudadano con sus datos provenientes de su credencial de elector, los datos de su domicilio en el extranjero, las claves de identificación para efectos de consulta, las imágenes digitalizadas de la credencial de elector y la constancia de domicilio y por último deberá aceptar los términos para el manejo de la información proporcionada, así como de su registro en la Lista Nominal Electoral. Artículos 275, 276.
- Actualizar la LNEE, almacenada en la Base de Datos de Registro (BDR). Artículo 277.
- Comprobar los datos del Ciudadano, obteniéndolos de la forma electrónica y comparándolos con los registrados en la Lista Nominal Electoral. Si son correctos, ingresar al Ciudadano a la LNEE y darlo de baja temporalmente de la LNE. Artículo 279.

- Generar el certificado digital y las llaves pública y privada para el Ciudadano aceptado en la LNEE.
- Consultar y/o modificar el registro del Ciudadano en la Lista Nominal Electoral, representada como la base de datos del Instituto Federal Electoral (BDIFE). Artículo 279.

4.2.2 Caso de uso consultar estado del trámite

Este caso de uso tiene como actor al Ciudadano y el servicio ofrecido es informarlo sobre la respuesta obtenida a la evaluación de su solicitud de registro.

En el Artículo 275, en el punto cinco, se indica que el Ciudadano interesado puede consultar a través de Internet o vía telefónica, el estado de su solicitud. En SEVI, la consulta del estado del trámite se convierte en obligatorio.

La justificación a lo anterior se refiere a que SEVI es un sistema ejecutado a través de Internet, motivo por el cual deben aplicarse las medidas de seguridad necesarias para el ejercicio del voto. Así, la principal tarea de este caso de uso además de informar la respuesta a la solicitud del Ciudadano, es proveerlo de la información necesaria para que al votar, SEVI pueda identificarlo y operar la captura del voto de manera segura.

La información a la que se hace mención no es más que el Certificado Digital del Ciudadano, requerido para la autenticación del mismo y el par de llaves pública y privada para mantener la transmisión segura de su voto. La seguridad se explicará en la última sección de este capítulo.

Las claves de identificación proporcionadas por el Ciudadano en el registro, permitirán la ubicación de su solicitud en el sistema. Las posibles respuestas que puede informar SEVI son las siguientes:

Solicitud Duplicada: si el Ciudadano a tratado de registrarse en más de una ocasión. La información válida para que pueda votar es la proporcionada en el primer registro.

Datos Inexistentes: si el registro del Ciudadano no es localizado en la Lista Nominal Electoral y por tanto no existen datos con que comparar los proporcionados por el Ciudadano.

Datos Erróneos: cuando al hacer la comparación de la información, algunos de los datos no coincide. Para la comparación se toma en cuenta toda la información de la credencial de elector, poniendo principal atención en la Clave de Elector, Nombre, Apellido Paterno, Apellido Materno, Estado Federal, Municipio y Sección del Ciudadano.

Solicitud Aceptada: cuando la información fue correcta y el Ciudadano ya ha sido ingresado a la Lista Nominal Electoral en el Extranjero. En este caso el Ciudadano debe descargar su Certificado Digital y sus llaves pública y privada. La descarga se refiere a dos archivos uno con extensión crt para el certificado y otro con extensión pem para las llaves. El Ciudadano puede guardar estos archivos en cualquier medio de almacenamiento. Hecho esto, se encontrará listo para emitir su voto en el periodo indicado por la ley.

4.2.3 Caso de uso votación

El servicio ofrecido por este caso de uso es la captura del voto emitido por el actor Ciudadano de forma segura.

El periodo abierto para que el Ciudadano pueda solicitar la emisión de su voto, es del 20 de mayo al 1ro de julio del año electoral. Artículo 284 y 288.

La boleta electoral electrónica (BEE) será generada al momento de solicitar la emisión del voto y después de haber sido debidamente

autenticado el Ciudadano e ingresado a la base de datos de autenticación (BDA). Artículo 283

Al presentar la BEE ante el Ciudadano, éste debe de marcarla dando click en el recuadro de su preferencia. El valor del voto va a procesarse una vez que el Ciudadano haya confirmado que su elección ha sido la correcta. Artículo 285.

Para asegurar la secrecía de su voto, el Ciudadano debe proporcionar al sistema su certificado digital y sus llaves pública y privada. Del lado del sistema, SEVI ejecutará el protocolo de seguridad en votaciones electrónicas basado en Lin-Hwang-Chang, a fin de transmitir el voto de manera segura. Artículo 286.

Al recibir el voto del Ciudadano, SEVI proporcionará un acuse de recibo al Ciudadano para hacer más eficiente la auditoria de su voto y almacenará la BEE en la base de datos de votación (BDV), la cual será registrada en la fecha recibida e indicando el distrito electoral y el estado federal al que pertenece el Ciudadano. Articulo 287.

4.2.4 Caso de uso generación de resultados

Este caso de uso tiene como función el conteo de los votos de manera automática, a las 18 horas del día 2 de julio del año electoral. Artículo 290.

Llegada la fecha y hora indicada, SEVI procederá al conteo de los votos. Para poder realizar esta tarea, la boletas electorales serán transmitidas y registradas de la BDV a la base de datos de conteo (BDC) dejando el valor del voto en claro y permitiendo así la suma de los votos idénticos. Artículo 291.

Como SEVI hace uso del protocolo de seguridad basado en Lin-Hwang-Chang, se tiene la posibilidad detectar al votante que emita su voto en más de una ocasión, incrementando la seguridad del sistema y la detección de fraude.

El resultado de la suma se desglosará por distrito electoral, según pertenezca el Ciudadano que emitió el voto. Artículo 292.

4.2.5 Caso de uso auditar voto

Servicio que ofrece al actor Ciudadano confirmar que su voto fue contabilizado.

SEVI entrega al Ciudadano un acuse de recibo que indica la recepción de su boleta electoral, entonces el Ciudadano podrá tener la opción de verificar que su voto fue contabilizado, revisando las listas de los ciudadanos votantes y localizando que su acuse de recibo se encuentra dentro de esa lista.

4.2.6 Caso de uso auditar distrito

Caso de uso que ofrece el servicio de escrutinio al actor Representante quien representa a los Ciudadanos encargados de observar el correcto funcionamiento del proceso electoral.

El Representante puede ser: funcionarios electorales de las mesas de escrutinio (Presidente, Secretario y Escrutador), consejero electoral, personal autorizado del Instituto Federal Electoral, representante de partido político por distrito electoral y administradores del sistema.

La auditoria distrital tiene dos fases: la primera es al término del registro entre el 30 de enero al 15 de mayo del año electoral, cuando los representantes de los partidos políticos verifican la Lista Nominal de Electores en el Extranjero, consultándola por distrito electoral o por el país de residencia del Ciudadano. Artículos 280, 281 y 282.

La segunda fase es al término de la votación y de la generación de resultados, los actores Representantes tendrán derecho de solicitar

reportes referentes a la lista de votantes, la lista de boletas electorales y la lista de votos válidos y nulos; así como los reportes de los resultados por partido en cada distrito electoral. Artículos 294 y 295.

Para la auditoria, cada Representante debe contar con sus claves de identificación para efecto de autenticación ante el sistema.

4.2.7 Caso de uso administración del sistema

Caso de uso donde el actor es el Administrador quien representa a los encargados de operar el sistema de manera interna, es decir, personal capacitado para realizar las tareas necesarias a fin de lograr el buen funcionamiento del sistema.

Entre las operaciones que pueden realizar los administradores, se encuentran el alta y la baja de las cuentas de los actores Representantes, la generación de reportes en cualquiera de las etapas del proceso electoral y mantenimiento en general de sistema.

Los administradores cuentan con restricciones, ya que ellos no pueden registrarse en la Lista Nominal de Electores en el Extranjero, solicitar y/o emitir su voto e interferir en el proceso de conteo. Sin embargo si pueden generar reportes directos del sistema de todos los reportes que pueden solicitar los actores representantes.

4.3 Diagrama de clases

El modelo de casos de uso aporta información para establecer las clases, objetos, atributos y operaciones. En base a lo anterior podemos pasar a la siguiente etapa que es la construcción del diagrama de clases.

La figura 4.3 muestra el diagrama de clases de SEVI en su modelo jerárquico, dividido en la interfaz con el usuario, el control o lógica y la comunicación y almacén.

Las clases Browser y CTRLI/O mantienen la comunicación entre el sistema y los actores Ciudadano, Representante y Administrador a través de ventanas de diálogo, formularios y avisos.

En la parte de Control, las clases Control Estación y Control Servidor, son las encargadas de delegar las tareas a las clases servicio, que son:

- Modulo IFE: clase encargada del registro, consulta y autenticación del Ciudadano.
- Casilla: clase encargada de la autenticación, votación y conteo de los votos.
- Consejo: clase encargada de la auditoria distrital y del Ciudadano del proceso.
- Seguridad: clase encargada de la activación del protocolo de seguridad a implementarse en SEVI.

De lado de las comunicaciones y el almacén, se encuentran los manejadores de bases de datos y los servidores de bases de datos, así como el protocolo de comunicación de red TCP/IP.

Se necesitan cinco bases de datos para cubrir los servicios funcionales, mismas que están distribuidas residentes en cuatro servidores, en el diagrama de clases son llamadas BDIFE, BDSR, BDSA, BDSV, BDSC, la primera corresponde a la base de datos del IFE y contiene la Lista Nominal Electoral, las restantes corresponden a los servidores de registro (SR), autenticación (SA), votación (SV) y conteo(SC), mas adelante se explicará a detalle la información que se almacena en cada una de ellas.

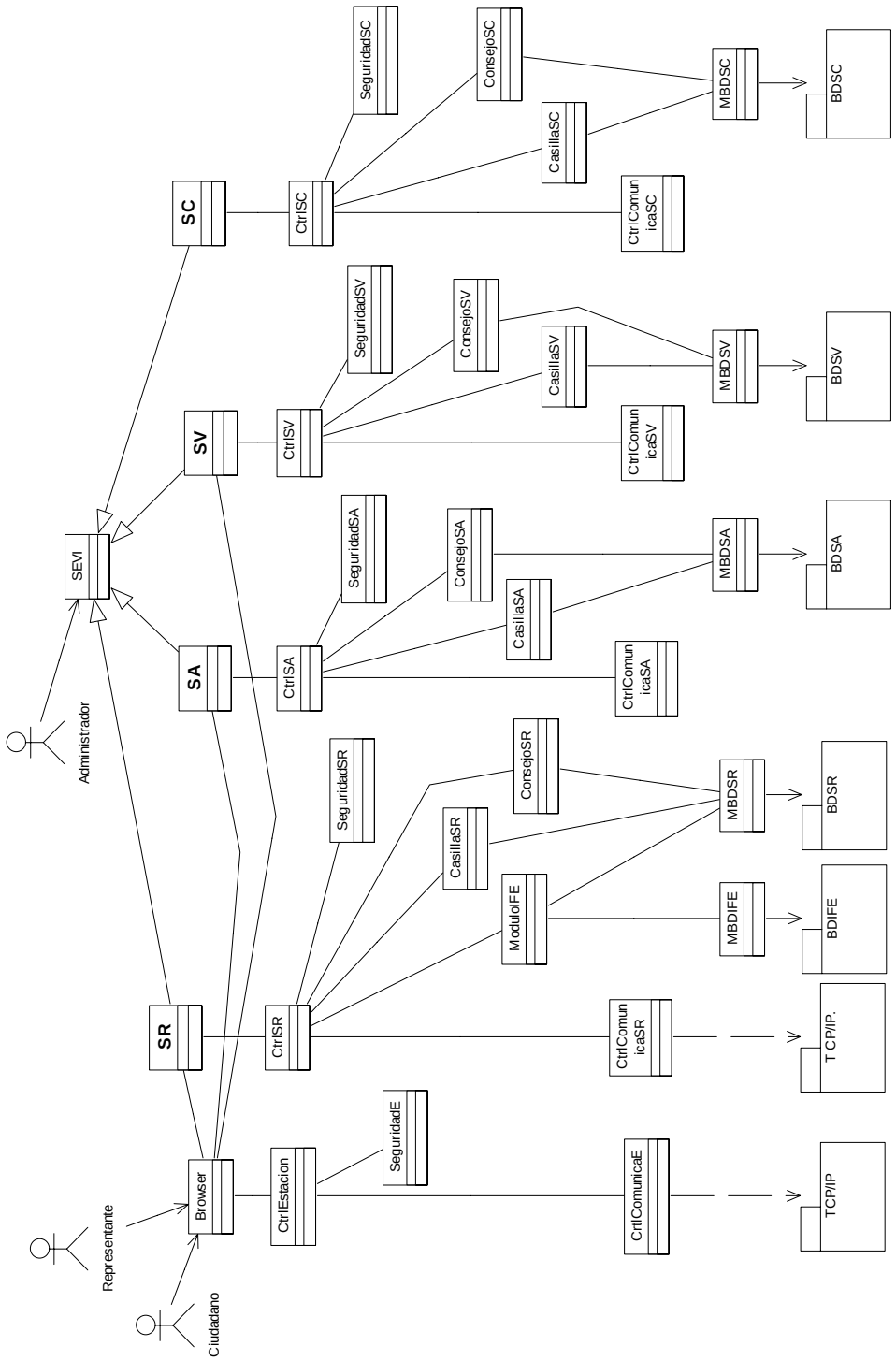


Fig. 4.3 Diagrama de clases para SEVI

4.4 Seguridad en SEVI

La funcionalidad de SEVI es conforme la ley electoral descrita en el COFIPE, sin embargo para brindar la seguridad debe implementarse un protocolo de seguridad para votaciones electrónicas.

Como se explicó en el capítulo 2 en el sistema SELES, se usó una variante del protocolo de seguridad de Lin-Hwang-Chang, éste protocolo puede ser implementado en SEVI ya que las tres fases de las que se compone cubren la seguridad en los casos de uso de votación y generación de resultados, el acuse de recibo dado a los votantes apoyaría a la auditoria para el caso de uso Auditar Distrito y Auditar Voto, por último el hecho de identificar votantes tramposos al emitir el voto, produce una mayor confianza al proceso, permitiendo la democracia en la elección.

A pesar de que el protocolo de seguridad cubre la mayor parte de los casos de uso, el caso de uso registro aún se conserva intacto y el proceso electoral comienza su operación precisamente con el registro. Para resolver este problema, se puede establecer un canal seguro entre la máquina cliente y la máquina servidor a través del protocolo para transferencia segura SSL (Secure Sockets Layer) [25].

Capítulo 5

Modelo de Diseño SEVI

El modelo de diseño es un modelo de objetos que describe la realización física de los casos de uso centrándose en cómo los requisitos funcionales y no funcionales, junto con otras restricciones relacionadas con el entorno de implementación, tienen impacto en el sistema, es decir, sirve como abstracción de la implementación del sistema y por lo mismo es utilizado como entrada fundamental de las actividades de implementación.

La presentación de cada caso de uso y el diagrama de clases, ilustran clases que no necesariamente se ejecutan sobre la misma máquina o computadora. SEVI va a implementarse sobre la arquitectura distribuida cliente/servidor, por tanto, sus clases se dividen entre las que se ejecutan en la máquina cliente y las que se ejecutan sobre la máquina servidor. Así, el diagrama de composición es el siguiente:

Fig. 5.1 Diagrama de Composición de SEVI

Antes de presentar el diagrama de clases refinado, para hacer más explicito los métodos y atributos utilizados en cada clase, se describen los protocolos usados para cubrir los servicios de seguridad y las bases de datos utilizadas.

5.1 Protocolos de seguridad

5.1.1 Basado en Lin-Hwang-Chang

El protocolo Lin-Hwang-Chang [7] en su versión mejorada [8], está basado en firmas a ciegas, protege la privacidad de los votantes y es capaz de detectar la duplicidad de los votos, originalmente utiliza el esquema de firma digital ElGamal, sin embargo se modifica este hecho y se sustituye por el esquema de firma digital DSA. Consta de tres fases: autenticación, votación y conteo, descritas a continuación.

Fase de Autenticación

Para poder emitir su voto, el votante debe identificarse con el servidor de autenticación (SA). Si la autenticación fue favorable, el SA firma a ciegas la petición del votante, con esto el votante puede comprobar que es un votante válido ante el servidor que reciba su voto.

Lo anterior se cubre cuando el votante solicita dos firmas a ciegas (z_1 y z_2) al SA. Las firmas a ciegas son basadas en el criptosistema de llave pública RSA y consisten en un mensaje *z* y un factor de opacidad u ocultamiento *b* cifrado con la llave pública del firmante (n_{sa}, e_{sa}).

Para el cálculo de z_1 y z_2 (ecuación 1), se utiliza la aritmética modular *mod p* y *mod q* de la firma digital DSA, de la forma $y = \alpha^a \bmod p$ y dos llaves privadas (*a* y k_1) elegidas por el votante.

$$z_1 = \left[\left(\alpha^{\,a} \bmod p\right) \times \left(b_1^{\,e_{SA}}\right)\right] \bmod n_{SA}$$
$$z_2 = \left[\left(\alpha^{\,k_1} \bmod p\right) \times \left(b_2^{\,e_{SA}}\right)\right] \bmod n_{SA} \qquad (1)$$

donde p y α son parámetros públicos DSA.

En esta fase, se utiliza una estampa de tiempo *t* y la firma digital f_v del votante para su autenticación. El mensaje enviado al SA es el siguiente:

$$\{V, SA, Cert_v, z_1, z_2, t, f_v\}$$

donde V es el votante, SA el identificador del servidor de autenticación y $Cert_v$ es el certificado digital del votante.

El SA recibe el mensaje y verifica la firma digital usando la llave pública del votante contenida en el $Cert_v$, si es correcta, el SA asigna un identificador único k_2 al votante, lo concatena con *t* y lo cifra con la llave pública del votante obteniendo z_3 (ecuación 2).

$$z_3 = \left(k_2 \parallel \mathrm{t}\right)^{\mathrm{e}_v} \bmod n_v \qquad (2)$$

Por último procede a realizar las firmas a ciegas solicitadas (3). En z_4 firma a z_1, en z_5 firma a z_2 y agrega una tercera z_6 para efecto de verificación.

$$z_4 = \left(z_1 \times SA\right)^{d_{SA}} \bmod n_{SA}$$
$$z_5 = \left(z_2 \times \left(\alpha^{\,k_2} \bmod p\right) \times SA\right)^{d_{SA}} \bmod n_{SA} \qquad (3)$$
$$z_6 = \left(\left(z_2\right)^2 \times \left(\alpha^{\,k_2} \bmod p\right) \times SA\right)^{d_{SA}} \bmod n_{SA}$$

Ahora el SA responde al votante enviando las firmas z_4, z_5 y z_6, sumando a cada una de ellas la estampa de tiempo y cifrándolas por separado con la llave pública del votante. El mensaje enviado es el siguiente:

$$\left\{SA, V, z_3, \left[\left(z_4 + t\right)^{e_v} \bmod n_v\right], \left[\left(z_5 + t\right)^{e_v} \bmod n_v\right], \left[\left(z_6 + t\right)^{e_v} \bmod n_v\right]\right\}$$

En el último paso de la primera fase, el votante recibe el mensaje y procede a descifrar con su llave privada a z_3, z_4, z_5 y z_6. Obtiene entonces su identificador único k_2 y hace el cálculo para obtener las firmas s_1, s_2 y s_3 de SA quitando el valor de ocultamiento en z_4, z_5 y z_6.

$$s_1 = z_4 \times (b_1)^{-1}$$
$$s_2 = z_5 \times (b_2)^{-1} \qquad (4)$$
$$s_3 = z_6 \times (b_2)^{-2}$$

Ahora s_1, s_2 y s_3 son las firmas que lo identificarán como votante válido frente al servidor de votación SV, quien tendrá como tarea confirmar que estas firmas fueron expedidas por el SA.

Fase de Votación

En esta fase el votante emite su voto, lo firma y lo envía al servidor de votación (SV).

Para que el votante firme su voto, sigue el proceso de la firma digital DSA, como llaves privadas se usaran a x_1 y x_2 y como llaves públicas a r_1 y r_2. El primer par se obtiene utilizando a k_1 y k_2, como se muestra en (5); el segundo par se calcula de la forma $(\alpha^k \bmod p) \bmod q$ según la ecuación 6:

$$x_1 = k_1 + k_2$$
$$x_2 = 2k_1 + k_2 \qquad (5)$$

$$r_1 = \left(\alpha^{\,k_1 + k_2} \bmod p\right) \bmod q$$
$$r_2 = \left(\alpha^{\,2k_1 + k_2} \bmod p\right) \bmod q \qquad (6)$$

Con las llaves privadas y públicas, ya puede obtenerse s_4 y s_5 que son las firmas del voto con módulo q, las ecuaciones en (7) muestran el cálculo, donde m es el voto y a la llave privada para DSA elegida por el votante en la fase de autenticación.

$$s_4 = (x_1)^{-1}(m + ar_1) \bmod q$$
$$s_5 = (x_2)^{-1}(m + ar_2) \bmod q \quad (7)$$

Hasta este punto, el votante cuenta ya con su voto firmado, el siguiente paso de esta fase es obtener los valores *l* y *pr*, con la finalidad de que el SV pueda verificar las firmas con módulo *q*. En pr_1 se encapsula el valor de l_1 y r_1, en pr_2 a l_2 y r_2 mediante el Teorema del Residuo Chino [24], las ecuaciones en (8) y (9) muestran el cálculo.

$$l_1 = \left[\left((\alpha^{k_1} \bmod p) \bmod n_{SA}\right) \times \left((\alpha^{k_2} \bmod p) \bmod n_{SA}\right)\right] \bmod n_{SA}$$
$$l_2 = \left[\left((\alpha^{k_1} \bmod p)^2 \bmod n_{SA}\right) \times \left((\alpha^{k_2} \bmod p) \bmod n_{SA}\right)\right] \bmod n_{SA} \quad (8)$$

$$pr_1 = \left[(r_1 \times n_{SA}) + (l_1 \times q)\right] \bmod (n_{SA} \times q)$$
$$pr_2 = \left[(r_2 \times n_{SA}) + (l_2 \times q)\right] \bmod (n_{SA} \times q) \quad (9)$$

Finalmente, el votante envía el mensaje llamado B, que es el boleto de votación al SV,

$$B = \{s_1, s_2, s_3, s_4, s_5, y, pr_1, pr_2, m\}$$

donde $y = \alpha^a \bmod p$, parámetro DSA.

Al llegar *B* al SV, éste verifica cinco firmas, tres provenientes del SA con módulo n_{sa} y dos que son del voto con módulo *q*. Las ecuaciones en (10) muestran la comprobación para las firmas módulo n_{sa}.

$$(SA \times y) \bmod n_{SA} = s_1^{e_{SA}} \bmod n_{SA}$$
$$\left(SA \times \frac{pr_1}{q}\right) \bmod n_{SA} = s_2^{e_{SA}} \bmod n_{SA} \quad (10)$$
$$\left(SA \times \frac{pr_2}{q}\right) \bmod n_{SA} = s_3^{e_{SA}} \bmod n_{SA}$$

Para verificar las firmas del voto módulo *q*, se debe obtener primero a r_1 y r_2, para eso se utiliza pr_1 y pr_2, según las ecuaciones en (11).

$$r_1 = \frac{pr_1}{n_{SA}} \bmod q$$
$$r_2 = \frac{pr_2}{n_{SA}} \bmod q \qquad (11)$$

Las ecuaciones en (12), resultan en *v*, si *v* es igual que r entonces las firmas son correctas. En el cálculo se usan los parámetros DSA α y *y*.

$$w = s^{-1} \bmod q$$
$$u_1 = wm \bmod q \qquad (12)$$
$$u_2 = rw \bmod q$$
$$v = \left(\alpha^{u_1} y^{u_2} \bmod p\right) \bmod q$$

Si la igualdad es positiva entonces, el SV acepta a B como válido, lo almacena y entrega al votante un acuse de recibo que avala su votación. Al término de la emisión de lo votos, el SV procede a enviarlos al servidor de conteo (SC), para la generación de los resultados.

Fase de Conteo

Última fase del protocolo de seguridad, en ella el SC recibe los boletos *B* válidos del SV, cuenta los que son idénticos y por única ocasión y obtiene el resultado final.

Para detectar la duplicidad en los boletos, el SC debe distinguir que tiene por lo menos dos de ellos con las mismas firmas, de la siguiente forma:

$$B_1 = \{s_1, s_2, s_3, s_4, s_5, y, pr_1, pr_2, m\}$$

$$B_2 = \{s_1, s_2, s_3, s_4', s_5', y, pr_1, pr_2, m'\}$$

Realizando las siguientes ecuaciones, se puede detectar al votante tramposo:

$$x_1 = \left(\frac{m' - m}{s_4' - s_4} \right) \bmod q \qquad (13)$$

$$x_2 = \left(\frac{m' - m}{s_5' - s_5} \right) \bmod q$$

$$k_1 = x_2 - x_1 \qquad (14)$$

$$k_2 = x_1 - k_1$$

El valor k_2, es el identificador único del votante para SA, por tanto, es posible identificar al votante que votó en más de una ocasión.

5.1.1.1 Implementación en SEVI

En el protocolo de seguridad se generan boletos de votación sólo con el valor del voto, para que al realizar el conteo se genere un resultado único. En SEVI es necesario presentar más de un resultado, la razón es por que la ley electoral nos indica que los votos deben contabilizarse por mesa de escrutinio correspondiente al distrito electoral al que pertenezca el Ciudadano votante. (Artículos 289-293 COFIPE).

Para la implementación de este protocolo en SEVI, es necesario modificar los mensajes que se transmiten entre el votante y los servidores y entre los servidores mismos ilustrados en la Fig. 5.2, con el fin no de mejorar el funcionamiento del protocolo, sino más bien para ajustarlo a la ley electoral.

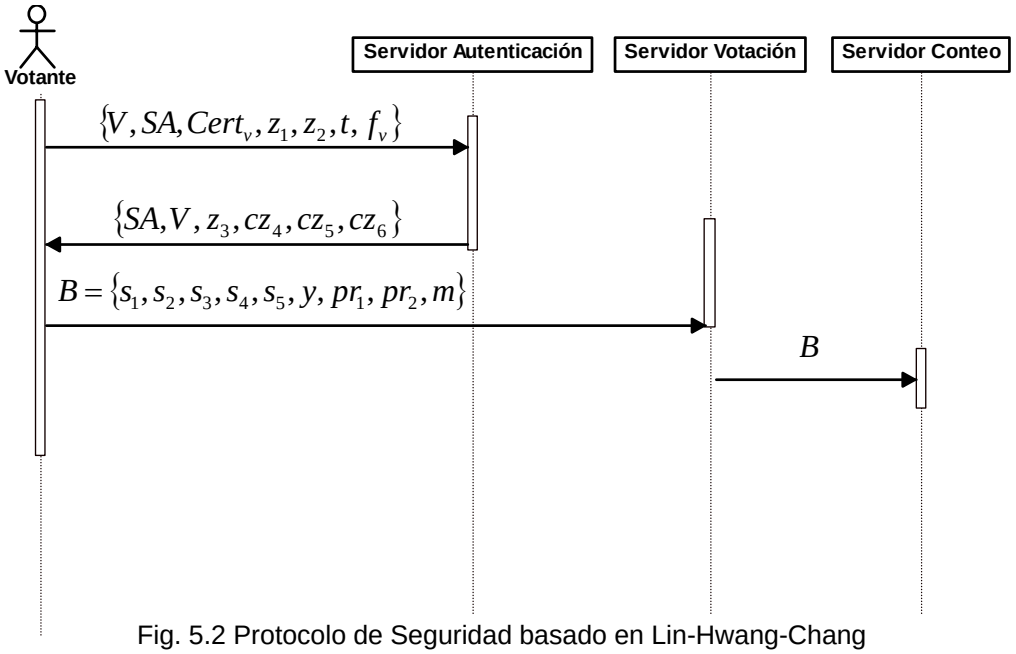


Fig. 5.2 Protocolo de Seguridad basado en Lin-Hwang-Chang

En SEVI el votante será el Ciudadano (que es nuestro actor) y el boleto de votación será la Boleta Electoral Electrónica (BEE) para seguir con la notación establecida en el modelo de casos de uso y de análisis.

El problema esencial en la implementación del protocolo de seguridad en SEVI es que se produzca un resultado por cada distrito electoral al que pertenezca el Ciudadano votante, lo que quiere decir que la BEE debe contener la información del distrito electoral a donde debe ser contabilizada. Esto se resuelve en la fase de autenticación.

El SA confirma la identidad del Ciudadano usando la firma digital y el certificado digital de éste. En ese momento puede solicitar la información del distrito electoral al Servidor de Registro, el cual contiene el registro completo del Ciudadano, así, en el mensaje de respuesta (que es la firma a ciegas solicitada), el SA puede adicionar el distrito electoral al que pertenece el Ciudadano. El mensaje enviado sería el siguiente:

$$\{SA, V, z_3, cz_4, cz_5, cz_{6,} de\ \}$$

donde *de* es el distrito electoral del Ciudadano.

Para que la BEE contenga el distrito electoral, basta con que el Ciudadano le ingrese la información, entonces la BEE tendrá la forma siguiente:

$$B = \{s_1, s_2, s_3, s_4, s_5, y, pr_1, pr_2, m, de\ \}$$

El SV al recibir la BEE verifica las cinco firmas y si son correctas la almacena en el distrito electoral correspondiente.

Al concluir la jornada electoral, el SV transmite al SC las BEE ahora por distrito electoral, para que al finalizar la transmisión, el SC sume los votos y genere los resultados por distrito electoral.

La Fig. 5.3 nos muestra el paso de mensajes tomando en cuenta el distrito electoral al que pertenece el Ciudadano.

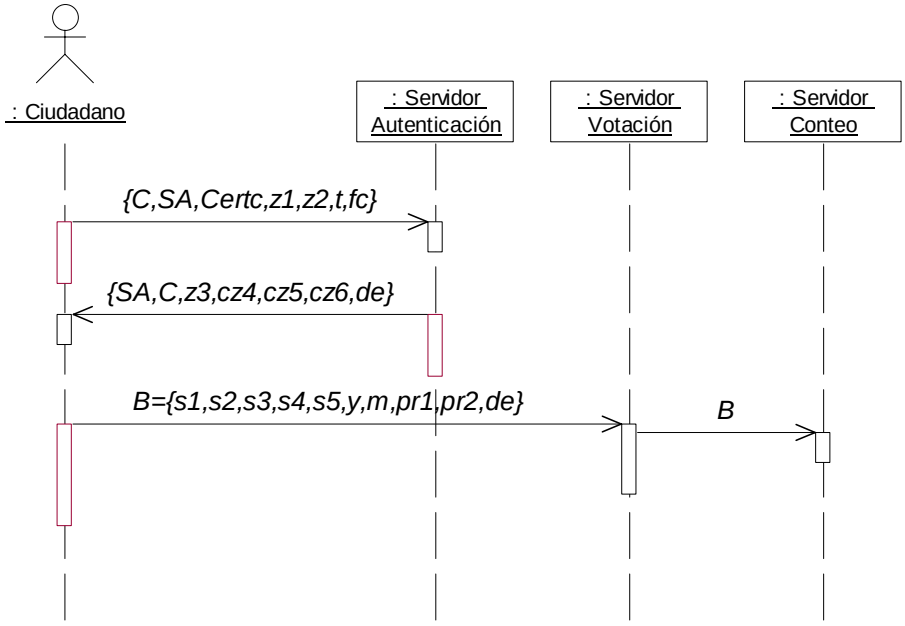


Fig. 5.3 Protocolo de seguridad basado en Lin-Hwang-Chang, ajustado a la ley electoral (COFIPE).

5.1.2 Protocolo de transmisión segura SSL (Secure Sockets Layer)

El protocolo SSL (Secure Sockets Layer) [25], se sitúa entre el protocolo de la capa de transporte (TCP/IP) y un protocolo de aplicación (http), prevé la comunicación segura entre el cliente y el servidor permitiendo la autenticación mutua, el uso de las firmas digitales para la integridad y el cifrado para la privacidad. En este proyecto se utiliza SSL en su versión 2, que es el primer protocolo de SSL y en la actualidad existen muchas puestas en práctica de esta versión.

Para poder aplicar este protocolo, primero debemos generar u obtener el certificado digital que avale nuestra identidad, debido a que no contamos con una Autoridad Certificadora que ratifique quienes somos, el certificado digital estará avalado por una firma generada por nosotros mismos, es decir, SEVI contará con un certificado generado y firmado por él mismo.

El protocolo SSL está diseñado para apoyar una gama de opciones para los diferentes algoritmos de criptografía, funciones resumen y firmas digitales, así podemos elegir el algoritmo adecuado para nuestra aplicación.

Dependiendo de la arquitectura donde está implementada la aplicación, se hará la configuración para que entre el servidor y cliente se establezca una sesión o canal seguro. La manera de establecerla puede ser variada dependiendo de si el servidor entrega un certificado o de si lo solicita al cliente.

Para establecer una sesión se hace por medio de un apretón de manos (handshake) entre el cliente y el servidor, el procedimiento se muestra en la figura 5.4.

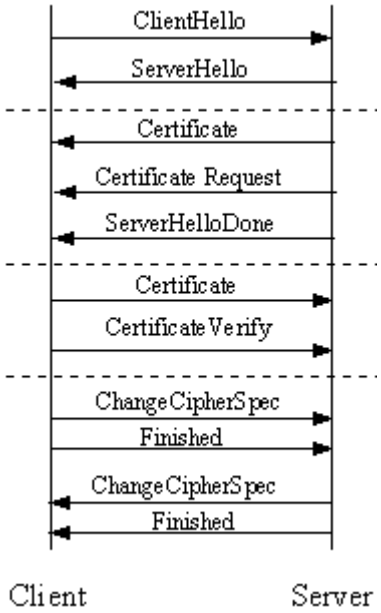


Fig. 5.4 Secuencia simplificada del handshake de SSL

Los elementos del handshake usados por el cliente y el servidor son:

1. Negociación de la forma de cifrado durante la transferencia de datos
    a. Método de intercambio de llaves, define como compartir la llave secreta usada por la aplicación en la transferencia de datos, el uso será convenido entre el servidor y el cliente, en SSLv2 el intercambio de llaves se hace para RSA solamente.
    b. Cifrado para la transferencia de datos, usa la criptografía convencional, hay nueve opciones:
        i. Ningún cifrado
        ii. Esquemas de Cifrado
            - RC4 con llaves de 40 bits

- RC4 con llaves de 128 bits

iii. Esquemas de bloque CBC (Cipher Block Chaining)

- RC2 con llave de 40 bits
- DES con llave de 40 bits
- DES con llave de 56 bits
- Triple-DES con llave de 168 bits
- Idea (llave de 128 bits)
- Fortezza (llave de 96 bits)

c. Funciones hash, se elige la función resumen para determinar como se obtendrán las firmas, soporta tres opciones:

- Sin firma
- MD5 128 bits
- SHA-1 160 bits

El resumen del mensaje se utiliza para crear el Código de Autenticación del Mensaje (MAC), el cual es cifrado con el mensaje para proveer integridad y prevenir los ataques de réplica.

2. Establecer y compartir una llave de sesión entre el servidor y cliente.
3. Autenticar el servidor al cliente (opcional)
4. Autenticar el cliente al servidor (opcional)

La secuencia de handshake usa tres protocolos:

1. El SSL Handshake Protocol, para realizar el establecimiento de la sesión SSL entre el cliente y el servidor.

2. El SSL Change Cipher Spec Protocol, para establecer el acuerdo en la negociación para la forma de cifrado,
3. El SSL Alert Protocol para transportar mensajes de error entre el cliente y el servidor.

Los protocolos y los datos del protocolo de aplicación son encapsulados en el protocolo de registro SSL.

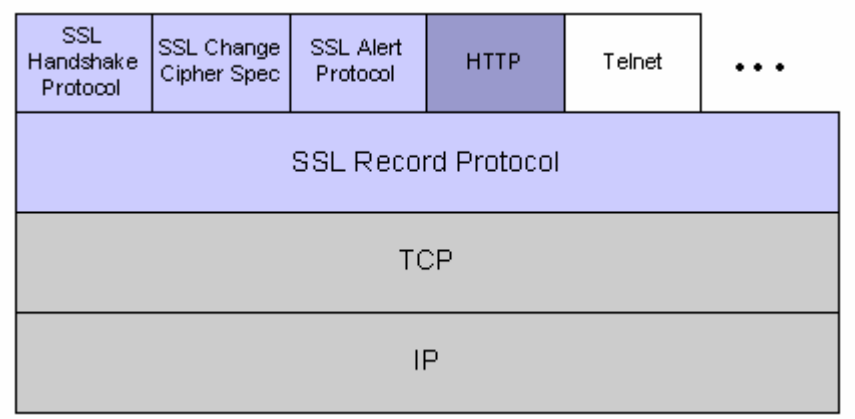


Fig. 5.5 Pila del protocolo SSL

La encapsulación de los protocolos de control de SSL por medio del protocolo de registro, significa que si se renegocia una sesión activa los protocolos de control serán transmitidos con seguridad.

El protocolo de registro SSL, se utiliza para transferir la aplicación y los datos de control de SSL entre el cliente y el servidor, posiblemente fragmentando los datos en unidades más pequeñas o combinando mensajes de datos múltiples del protocolo de alto nivel en unidades particulares.

Un uso común de SSL es asegurar la comunicación del http del web entre un navegador y el web server. La versión segura es principalmente http sobre SSL llamado https y utiliza el puerto 443.

El protocolo SSL es usado en SEVI para establecer una conexión segura entre sus usuarios (Ciudadano, Representante) y los servidores con los que se comunica (Registro, Autenticación y Votación).

5.2 Bases de datos

Las bases de datos utilizadas se encuentran en sus servidores de bases de datos, SEVI cuenta con cuatro servidores:

- Servidor de Registro (SR): donde se desarrolla el proceso de registro.
- Servidor de Autenticación (SA): consiste en autenticar al Ciudadano y proporcionarle su boleta electoral.
- Servidor de Votación (SV): su tarea es recibir las boletas electorales y verificar que fueron expedidas por el SA, para considerar el voto como válido o nulo.
- Servidor de Conteo (SC): en él se realiza la generación del resultado, una vez que recibe las boletas electorales por parte del SV.

El funcionamiento de SEVI, requiere la utilización de cinco bases de datos:

- BDIFE: Lista Nominal de Electores.
- BDSR: utilizada por el servidor de registro, almacena la Lista Nominal de Electores en el Extranjero
- BDSA: utilizada por el servidor de autenticación, almacena la Lista Nominal de Electores en el Extranjero autenticados.
- BDSV: utilizada por el servidor de votación, almacena las boletas electorales válidas y nulas.

- BDSC: utilizada por el servidor de conteo, almacena las boletas electorales válidas, para realizar el conteo final.

5.2.1 Diagramas entidad-relación

Base de datos IFE (BDIFE)

Esta base de datos contiene a la Lista Nominal de Electores (LNE). Actualmente en el IFE cuentan con dos centros de información, la matriz se ubica en el estado de Pachuca y su respaldo en el Distrito Federal.

Esta base de datos está formada por sólo una tabla (Fig. 5.6) que contiene los datos electorales del Ciudadano.

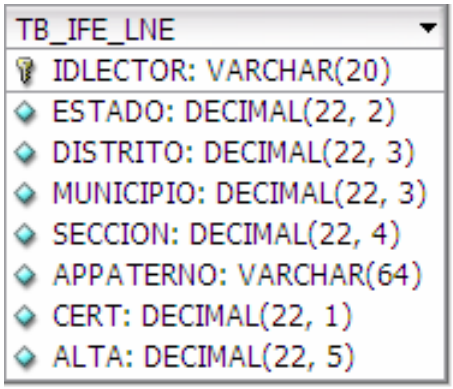


Fig. 5.6 Diagrama E-R base de datos IFE

La principal operación ofrecida es consultar la existencia del Ciudadano y una vez registrado en la lista nominal de electores en el extranjero, la baja temporal del mismo, para darse de alta nuevamente al término del proceso electoral.

Base de datos SR (BDSR)

En esta base de datos se almacenan los registros de los ciudadanos para obtener la Lista Nominal de Electores en el Extranjero (LNEE). Está compuesta por cuatro tablas mostradas en la Fig. 5.7. La descripción de las tablas es la siguiente:

TB_SEV_DP: contiene la información personal y electoral del Ciudadano.

TB_SEV_DEXT: contiene la información correspondiente al domicilio en el extranjero.

TB_SEV_PASS: contiene la información para la identificación del Ciudadano.

TB_SEV_IMG: contiene la referencia de los archivos de imagen de la credencial de elector y la constancia domiciliaria del Ciudadano.

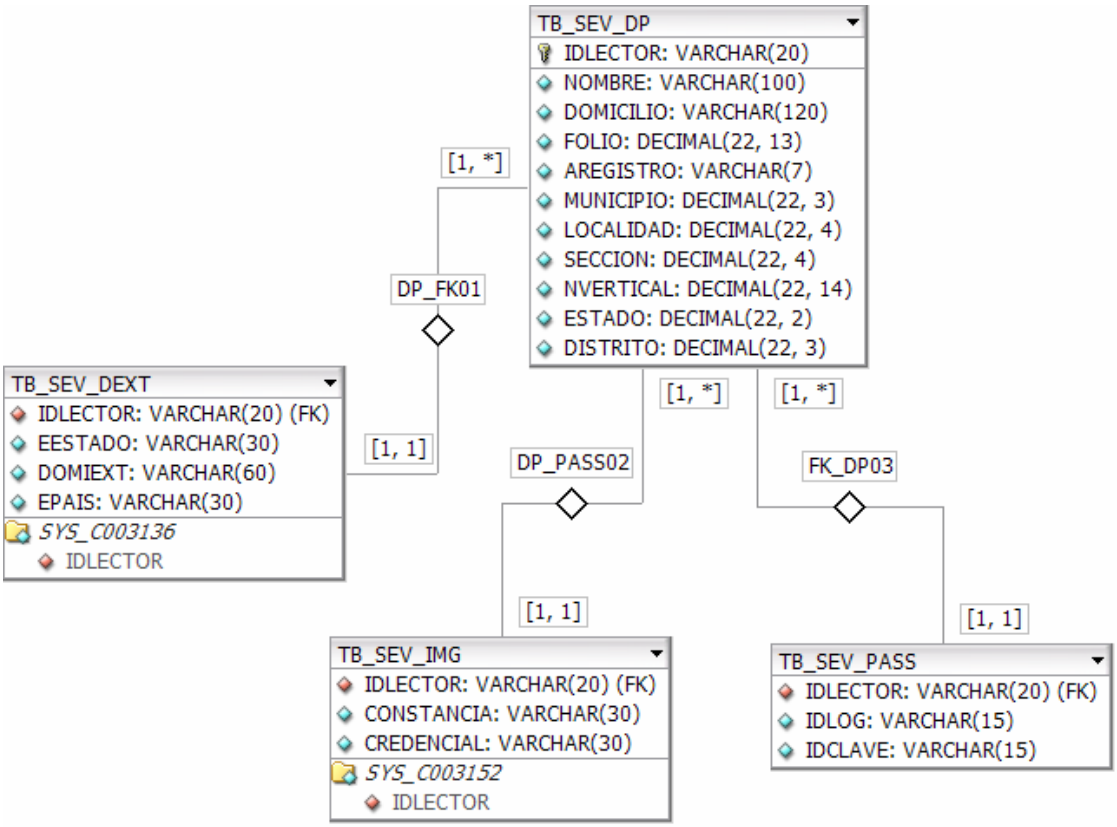


Fig. 5.7 Diagrama E-R base de datos SR

Base de datos SA (BDSA)

Base de datos que contiene una sola tabla presentada en la Fig. 5.8, en la cual se almacena el identificador único del votante, generado al realizarse la autenticación, el distrito electoral y la entidad federativa a la que pertenece el votante y la estampa de tiempo capturada al momento de solicitar la autenticación.

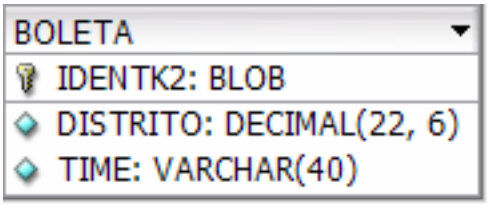


Fig. 5.8 Diagrama E-R base de datos SA

Base de datos SV (BDSV)

Base de datos compuesta por cuatro tablas mostradas en la Fig. 5.9, es utilizada para almacenar las boletas electorales válidas y la información referente a los actores Representantes y al distrito electoral al que pertenecen. La descripción de sus tablas es la siguiente:

TB_URN_D: almacena el código y el nombre de los distritos electorales a nivel nacional.

TB_URN_PASS: contiene las claves de acceso de cada actor Representante.

TB_URN_DP: contiene los registros actores Representantes.

BOLETAS: en ella se depositan las boletas electorales válidas, provenientes de los votantes.

Esta base de datos, será la encargada de recibir los votos de los ciudadanos, así como los registros de los actores Representantes que son los que tienen derecho a realizar la auditoria de la información, en las distintas etapas del proceso electoral.

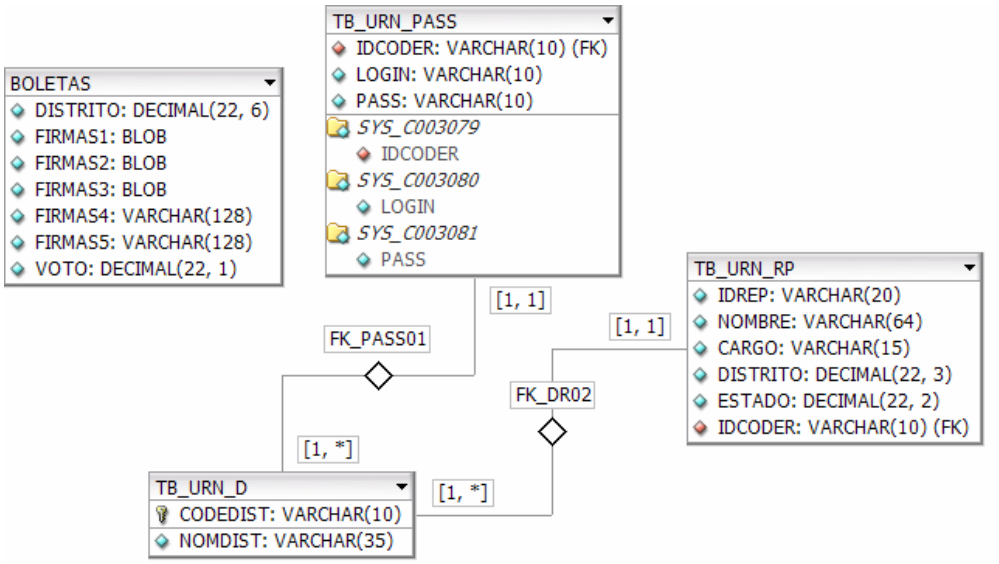


Fig. 5.9 Diagrama E-R base de datos SV

Base de datos SC (BDSC)

Base de datos que recibe las boletas electorales válidas provenientes del SV, está compuesta por tres tablas independientes ilustradas en la Fig. 5.10. La descripción de las tablas en la siguiente:

Boleta: en ella se almacenan las boletas electorales tal cual llegan del SV, el valor del voto contenido en la boleta y el distrito electoral al que pertenece el voto.

Contador: tabla en donde se registran los resultados de la votación, como es el total de los votos emitidos, el total de boletas recibidas, el número de votos válidos y el número de votos nulos.

Votante: contiene el identificador, nombre y distrito al que pertenece el votante tramposo que voto en más de una ocasión.

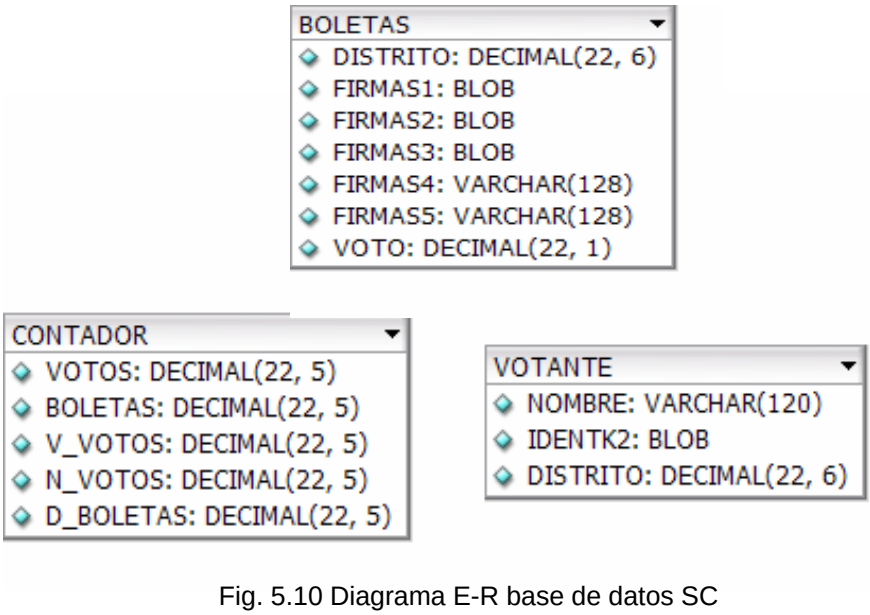


Fig. 5.10 Diagrama E-R base de datos SC

5.3 Diagrama de clases refinado

Debido a lo extenso del diagrama de clases refinado, presentaremos las clases mostrando sus métodos y atributos, así como sus diagramas se secuencia, para cada caso de uso por separado.

Caso de Uso Registro

El Diagrama de Clases para el registro se muestra en la Fig. 5.11, está compuesto de nueve clases, tres ejecutadas desde la máquina cliente del Ciudadano y seis ejecutadas desde la máquina servidor del SR.

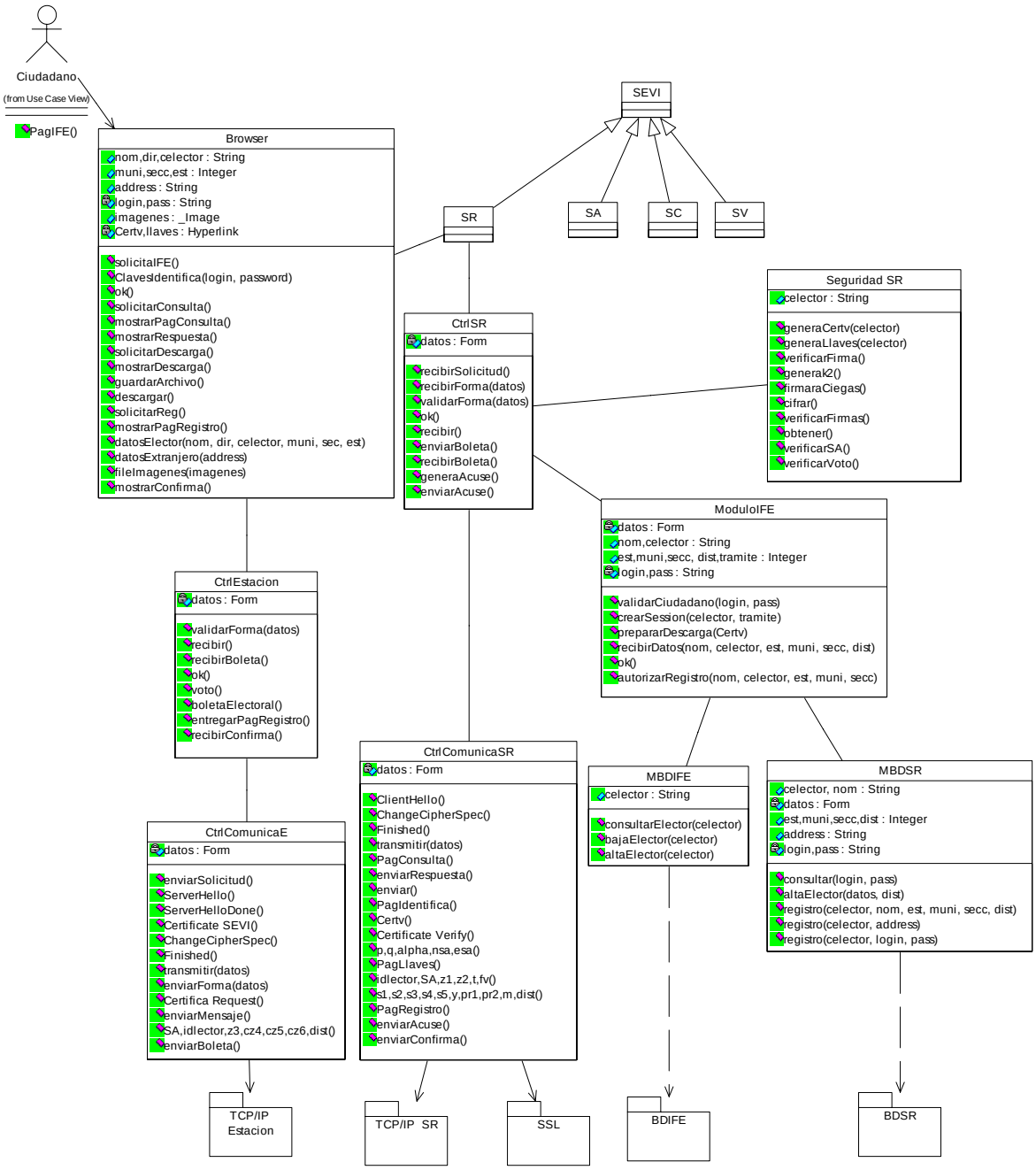


Fig. 5.11 Diagrama de clases refinado caso de uso registro.

La clase Modulo IFE es la encargada de realizar las verificaciones correspondientes a la identidad del Ciudadano, por medio de la comparación entre la información proveniente del cliente a través de la forma de registro, validada desde el navegador con la ayuda de la clase Browser y del registro de la base de datos de la Lista Nominal de Electores (BDIFE). Si la comparación es idéntica se procede a dar de alta al Ciudadano en la base de datos de registro (BDSR), dándolo de baja temporalmente de la BDIFE.

El diagrama de secuencia para este caso de uso, ilustra los mensajes entre las clases en la Fig. 5.12

El Ciudadano solicita su registro y se establece un canal seguro para la transmisión de los datos, una vez terminada la captura de la información, se envía al SR y después de hacer algunas evaluaciones, le confirma al Ciudadano la recepción de sus datos.

Internamente SEVI llama al método autoriza registro para confirmar la validez del usuario y decidir aceptarle o rechazarle.

Si el Ciudadano fue aceptado, el SR genera su certificado digital que lo avalará ante el SA y sus llaves (pública y privada) para la protección de su voto, esta tarea se le delega a la clase Seguridad Servidor.

El registro estará abierto a los Ciudadanos el periodo indicado en la ley, una vez cumplida la fecha última de registro, el SR no recibirá ninguna solicitud.

Caso de uso consultar estado del trámite

Una vez recibida la información del Ciudadano, éste tiene que confirmar si fue aceptado o no, por tanto solicita la consulta del estado de su trámite y SEVI requiere de sus claves de identificación para localizarle en el SR.

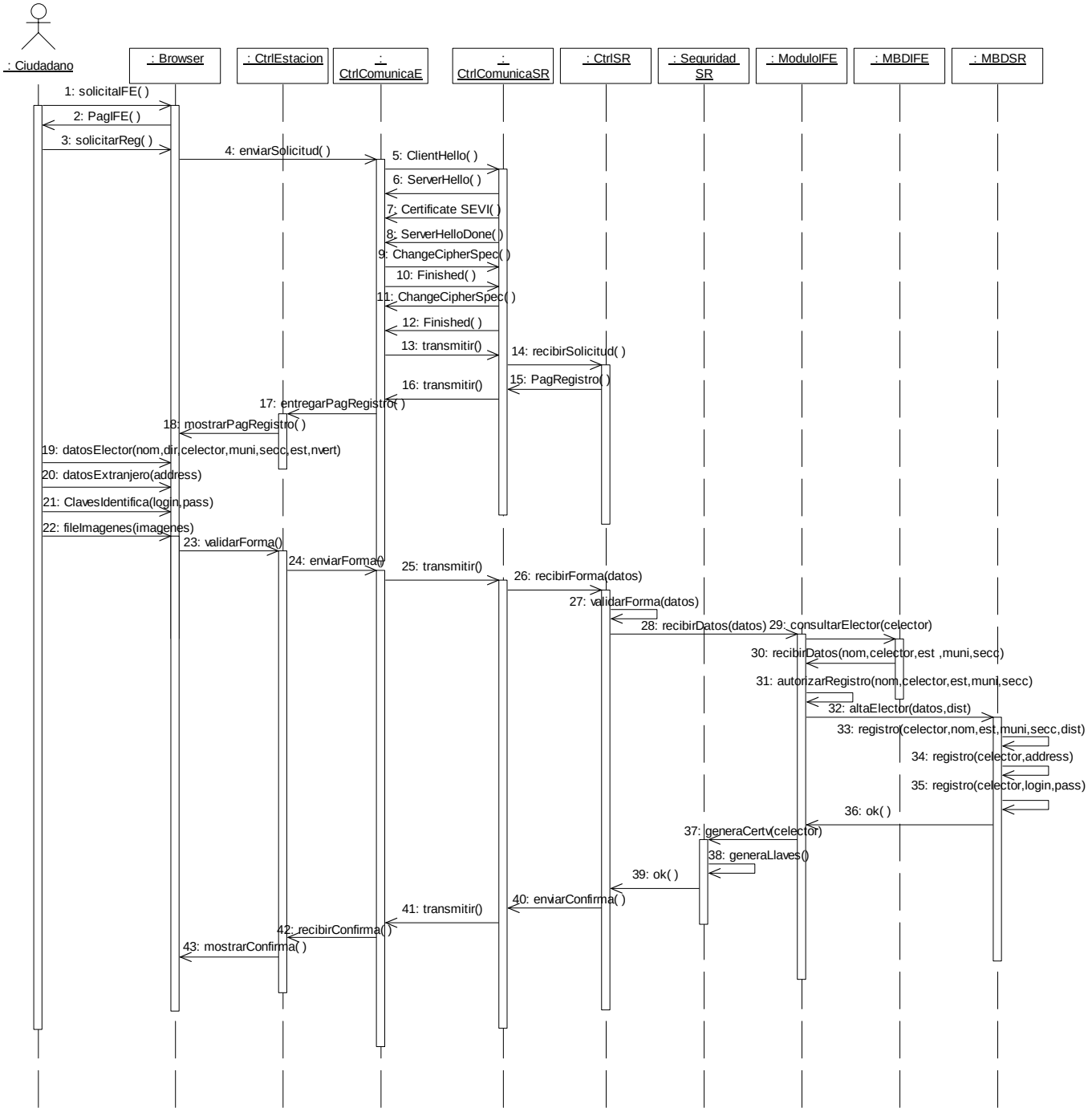


Fig. 5.12 Diagrama de secuencia para el registro del Ciudadano.

El diagrama de clases refinado de la Fig. 5.13, contiene las clases para el caso de uso Consultar el Estado del Trámite. El diagrama de secuencia ilustrado en la figura 5.14 sigue el caso en el que el Ciudadano proporcionó su información de manera correcta y fue aceptado en la Lista Nominal de Electores en el Extranjero (LNEE).

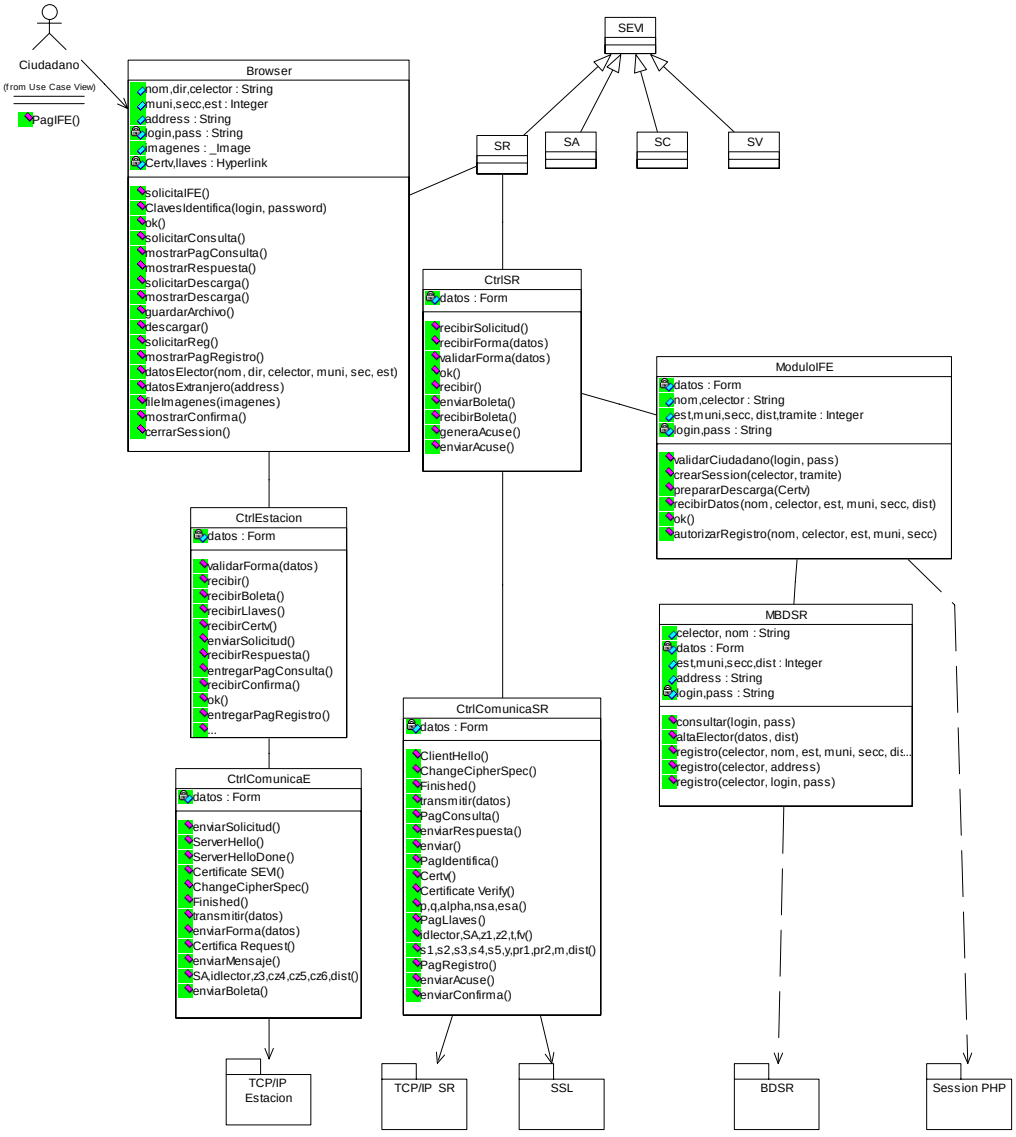


Fig. 5.13 Diagrama de clases refinado consulta estado del trámite.

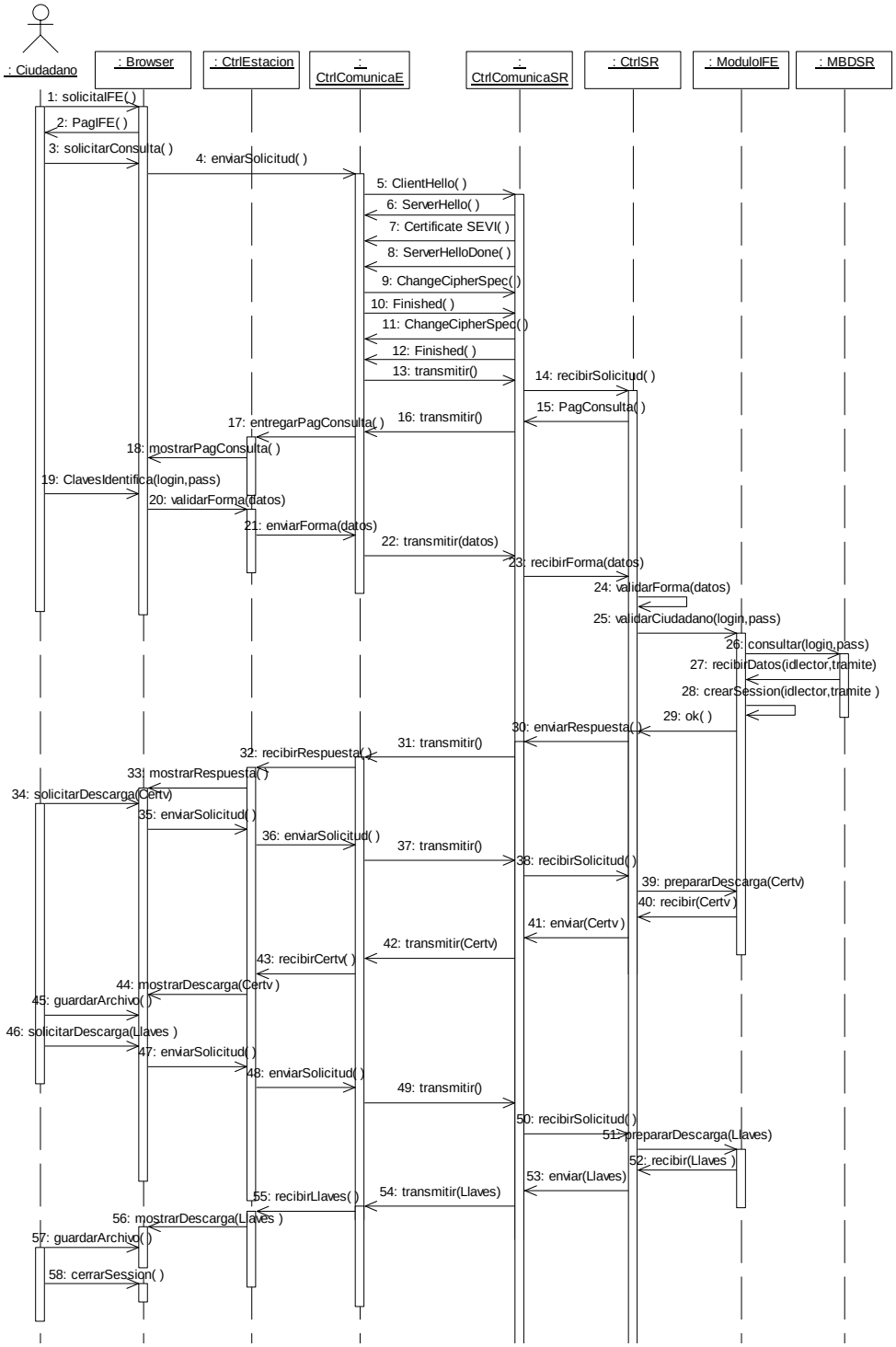


Fig. 5.14 Diagrama de secuencia consulta estado del trámite.

Sin embargo puede haber cuatro tipos de respuestas que son las siguientes:

- Ciudadano Rechazado por datos incorrectos: cuando la comparación entre los registros del IFE y los proporcionados por el usuario resulto distinta, en este caso el Ciudadano puede volver a registrarse con sus datos correctos.
- Ciudadano Rechazado por Registro Inexistente: el Ciudadano no fue localizado en la lista nominal de electores, lo que quiere decir que no cuenta con su credencial de elector vigente.
- Ciudadano Rechazado por Duplicidad: mensaje que indica al Ciudadano que ya existe un registro de el que fue aceptado y que no van a contemplarse los registros posteriores a este.
- Ciudadano Aceptado: cuando el Ciudadano proporciono de manera correcta la información y se le permite votar. Se le solicita descargue su certificado digital y su par de llaves (pública y privada), para efecto de votación segura.

Hasta este punto, el Ciudadano ya esta listo para votar, tiene en su poder lo necesario para identificarse y emitir su voto, que es su alta en la LNEE, su certificado digital y sus llaves pública y privada.

Caso de uso votación

Llegado el periodo para la emisión de los votos estipulado en la ley, el servidor de votación (SV) se pone en servicio para los Ciudadanos que emitan su voto. SEVI asegura la emisión ejecutando en este periodo el protocolo de seguridad basado en Lin-Hwang-Chang en sus dos primeras fases (Autenticación y Votación).

El diagrama de clases para este caso de uso se muestra en la Fig. 5.15.

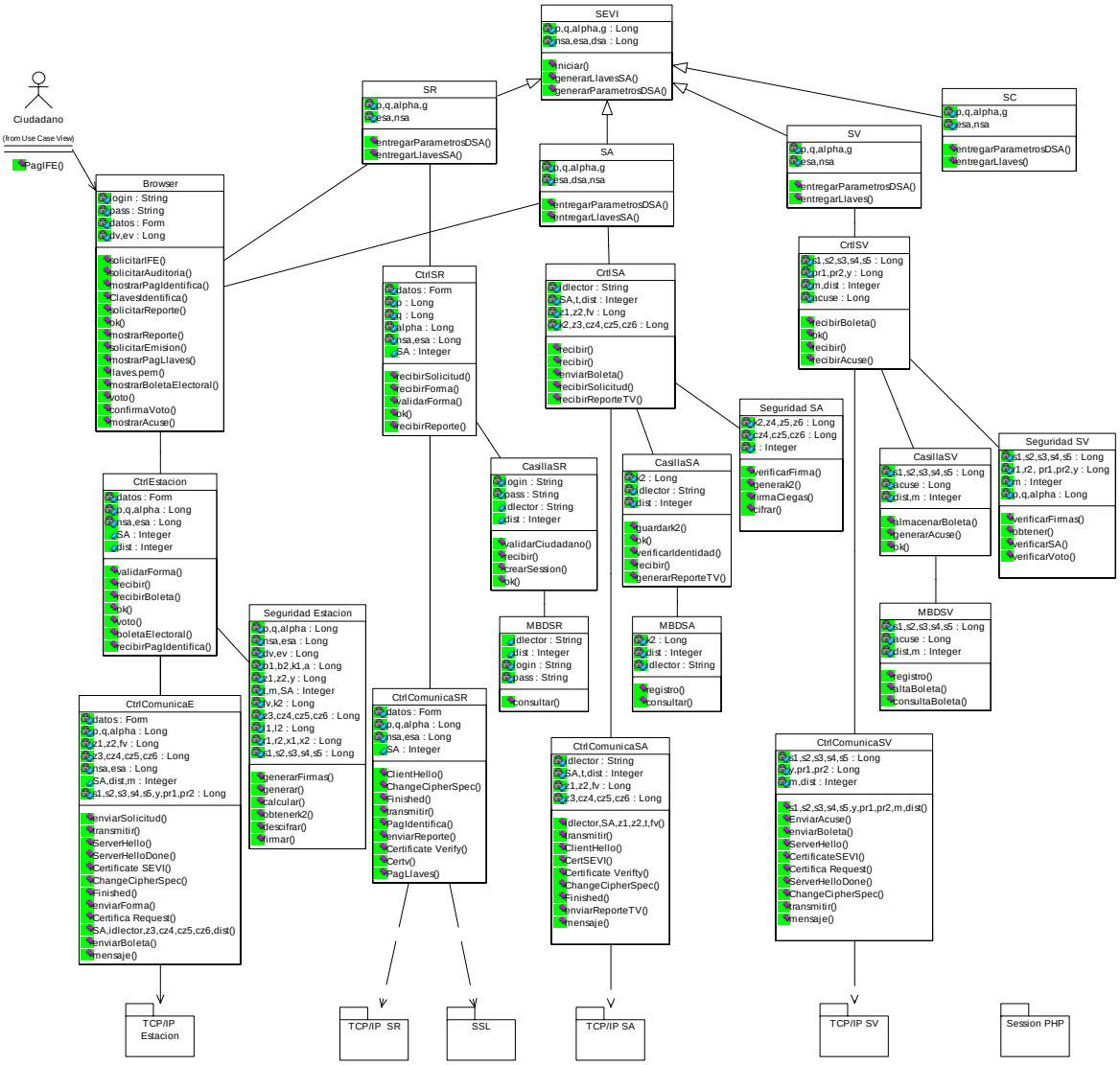


Fig. 5.15 Diagrama de clase refinado caso de uso votación.

Para poder emitir su voto, el Ciudadano debe primero identificarse ante el SR a través de la clase Casilla y generar así la sesión que permitirá el paso de los mensajes entre el servidor y el cliente. Previamente, la clase Seguridad Servidor genera los parámetros DSA *(p,q,alpha)* y las llaves pública y privada del SA

(nsa,dsa,esa), estos datos son necesarios para las firmas digitales y el cifrado de la información que se transmite.

Dado que no contamos con una Autoridad Certificadora que nos permita publicar los parámetros y las llaves públicas del SA, ésta información es manipulada a través de la sesión generada para el Ciudadano, la Fig. 5.16 muestra la secuencia de los mensajes.

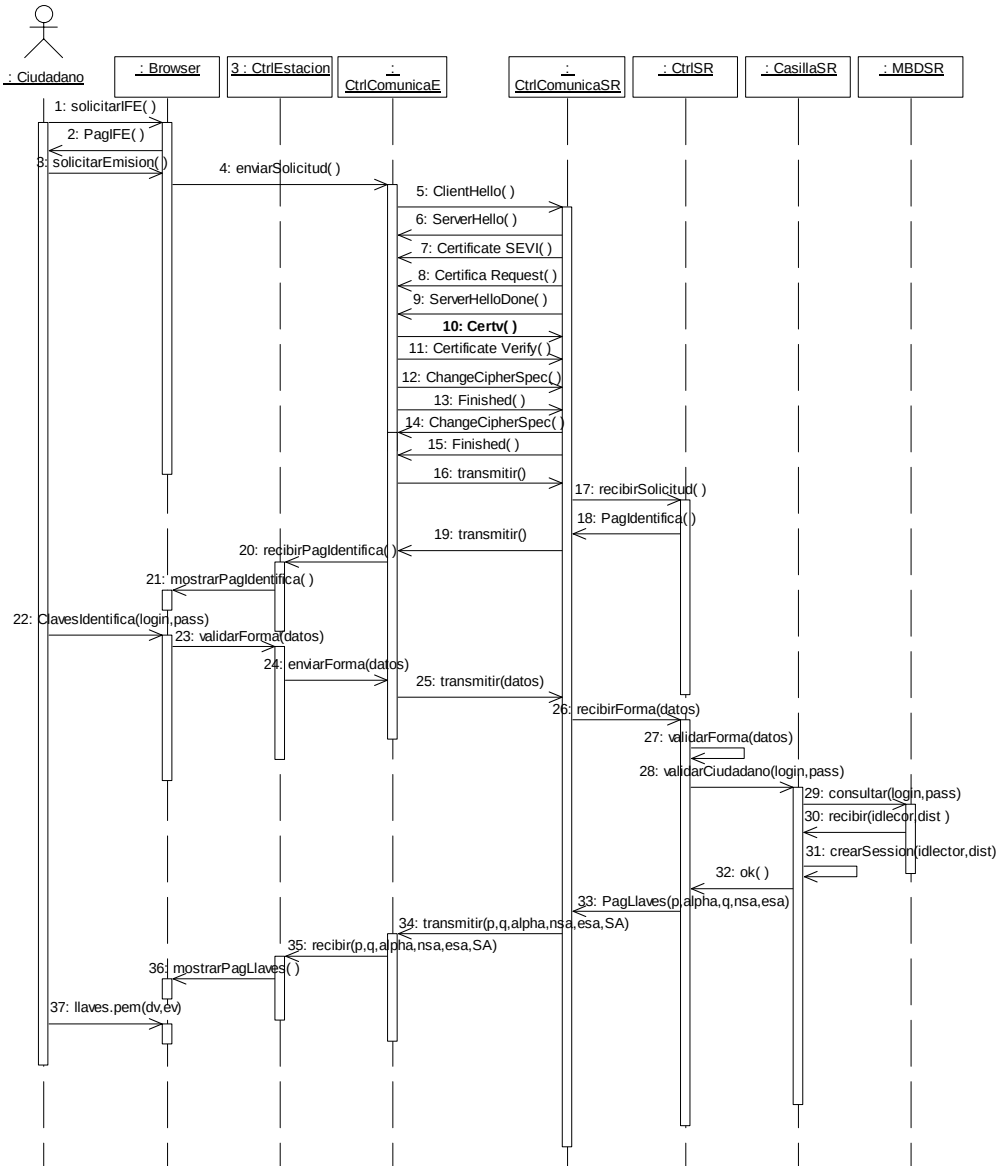


Fig. 5.16 Diagrama de Secuencia Votación (Parte 1).

Continuando con el diagrama de secuencia de la votación en SEVI, una vez que sea creada la sesión del Ciudadano, éste se convierte en votante y para poder realizar los cálculos respectivos para solicitar las firmas a ciegas, debe proporcionar su llave privada. Hecho lo anterior, la clase Control Estación está lista para los calculos. Cuenta con los parámetros DSA *(p,q,alpha)*, la llave pública del SA *(esa,nsa)*, su llave privada (*dv)*, su llave pública *(ev)* contenida en $Cert_v$; genera los factores de opacidad *(b_1 y b_2),* los números aleatorios *(a y k_1)* y la estampa de tiempo *(t)*; calcula las firmas *(z_1, z_2 y f_v),* por último envía el mensaje de solicitud para la firma a ciegas al SA.

El SA recibe el mensaje, verifica la f_v usando la *ev* contenida en $Cert_v$, si es correcta, genera el identificador único k_2 para el votante y lo almacena en la base de datos del servidor de autenticación; firma a ciegas *(z_4,z_5,z_6)* y para enviar el mensaje de respuesta cifra con *ev* a k_2, z_4,z_5 y z_6 obteniendo z_3,cz_4,cz_5 y cz_6 respectivamente.

Llegando el mensaje al votante, obtiene su identificador y las firmas descifrándolas con su llave privada, para terminar con la fase de autenticación, hace el cálculo para obtener las firmas reales del SA (*s_1, s_2 y s_3)*. El diagrama de secuencia (parte 2) se ilustra en la Fig. 5.17.

Entramos ya a la fase de votación, el votante ya emitió su voto. La clase seguridad estación firma el voto *(s_4 y s_5)*, construye la boleta electoral generando *B* y la envía al SV.

Al recibir la boleta electoral el SV verifica las cinco firmas que vienen contenidas en ella (tres del SA y dos del voto), si es correcta la verificación almacena la boleta electoral en la base de datos de votación y entrega al Ciudadano votante su acuse de recibido. El diagrama de secuencia en la Fig. 5.18 muestra la última parte del caso de uso votación.

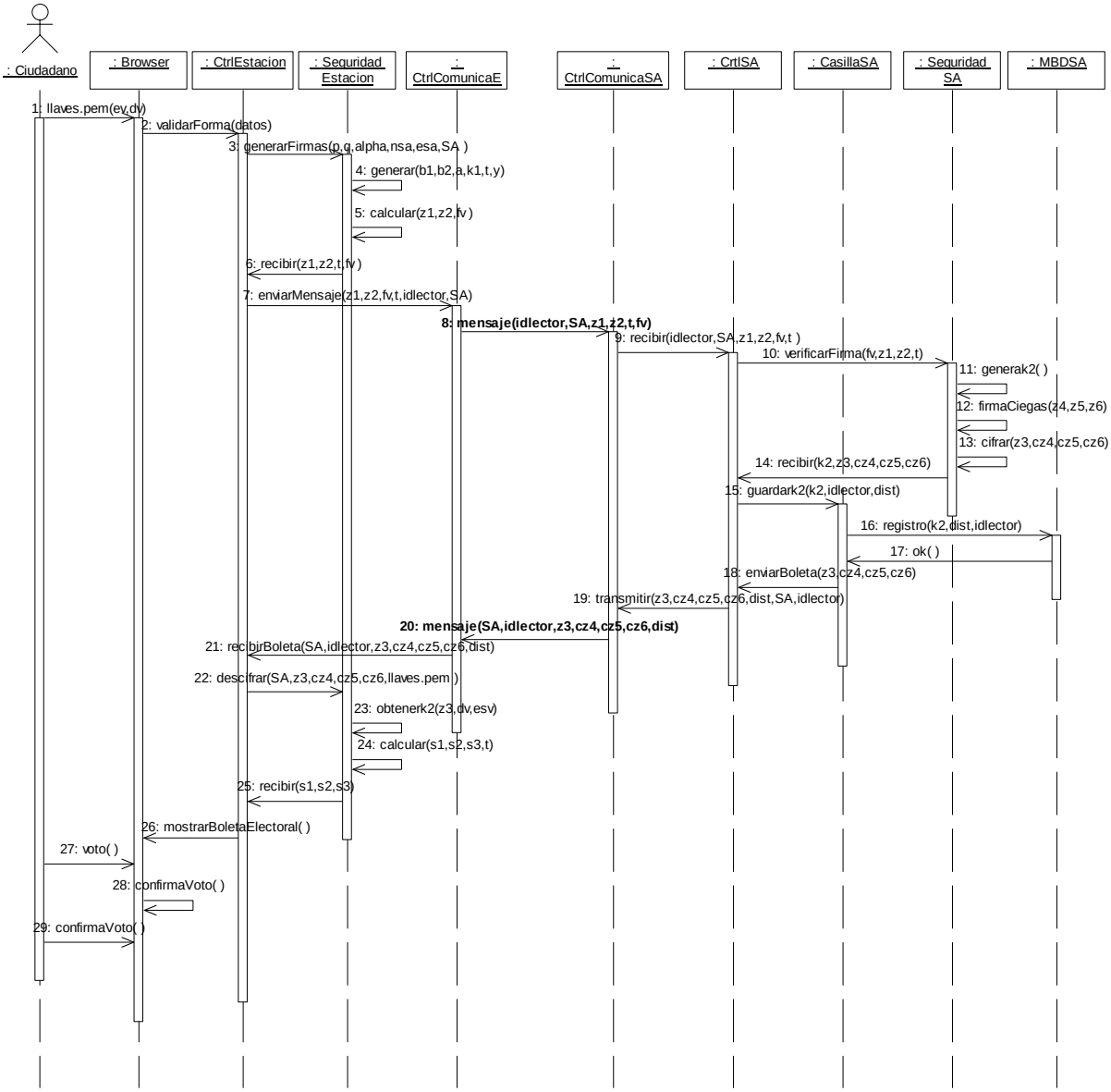


Fig. 5.17 Diagrama de secuencia votación (Parte 2).

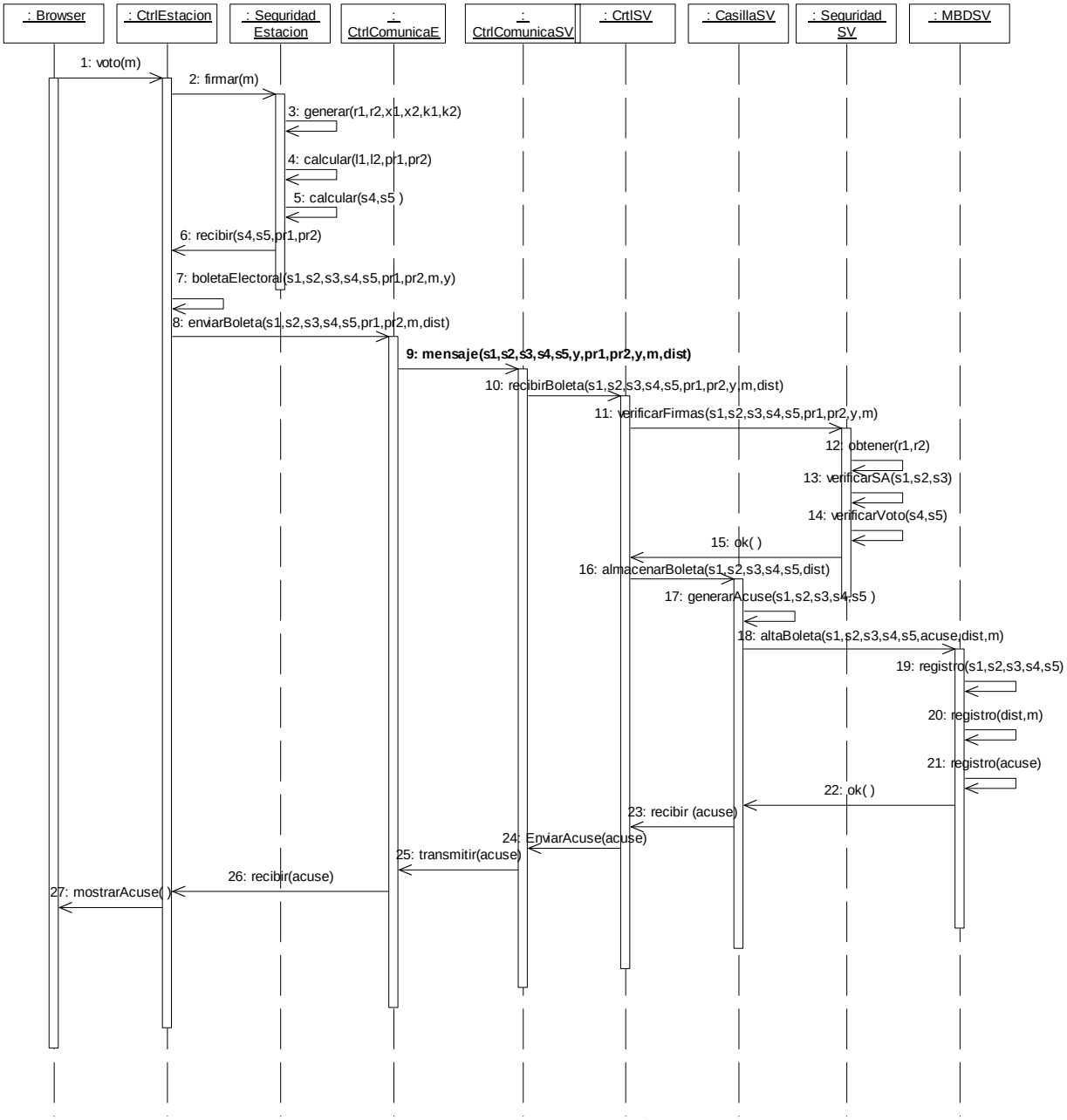


Fig. 5.18 Diagrama de secuencia votación (Parte 3).

Caso de uso generación de resultados

La Fig. 5.19 muestra el diagrama de clases refinado para este caso de uso.

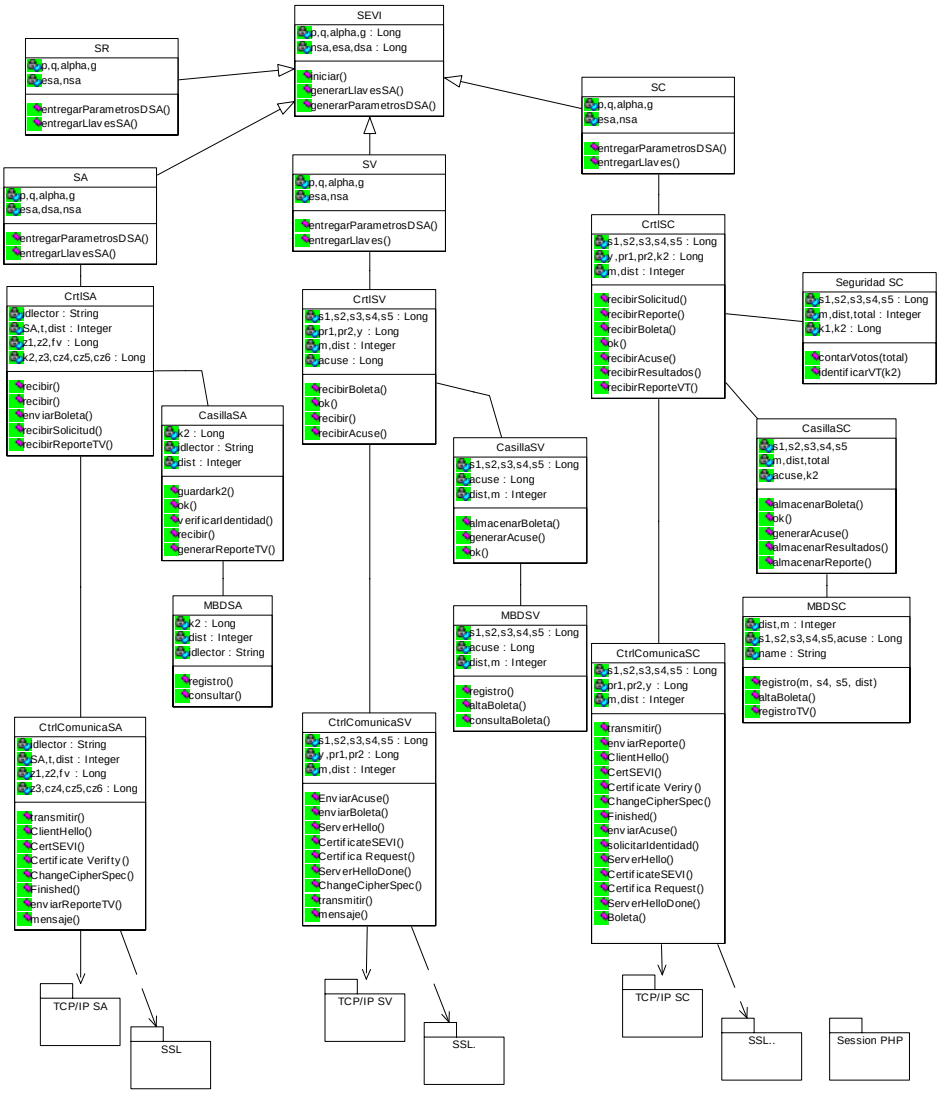


Fig. 5.19 Diagrama de Clases Refinado Generación de Resultados.

Este caso de uso cuenta los votos provenientes del SV llegada la hora del escrutinio indicada en la ley electoral. Al término de la

jornada electoral, el SV envía las boletas electorales al SC y recibe un acuse de recibo por la transacción. La Fig. 5.20 muestra el diagrama de secuencia del paso de mensajes entre el SV y el SC.

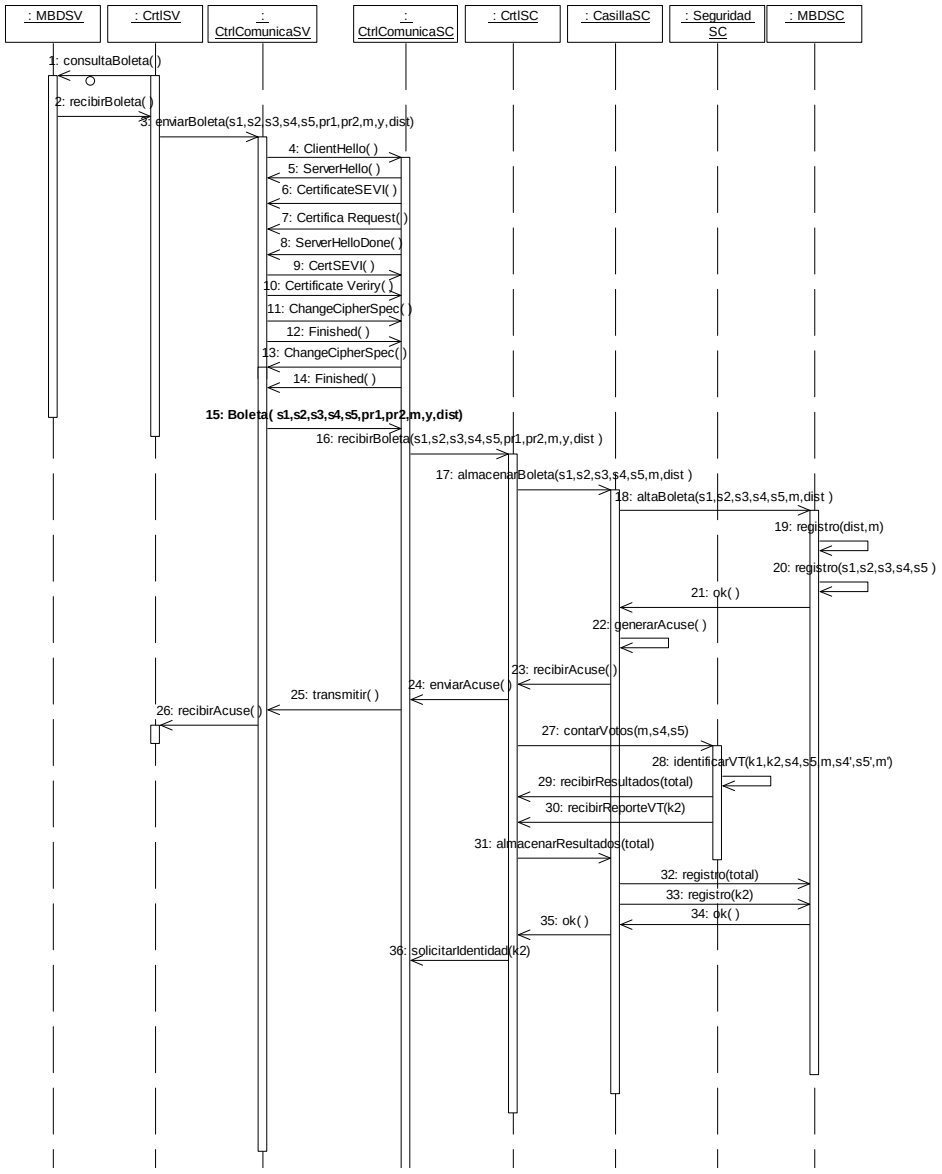


Fig. 5.20 Diagrama de secuencia generación de resultados.

El SC realiza la suma de los votos idénticos y corrobora que no se trate de un votante tramposo comparando una a una las boletas electorales.

Al final reporta los resultados y solicita las identidades de los votantes tramposos al SA. La Fig. 5.21 muestra el paso de mensajes entre el SC y el SA.

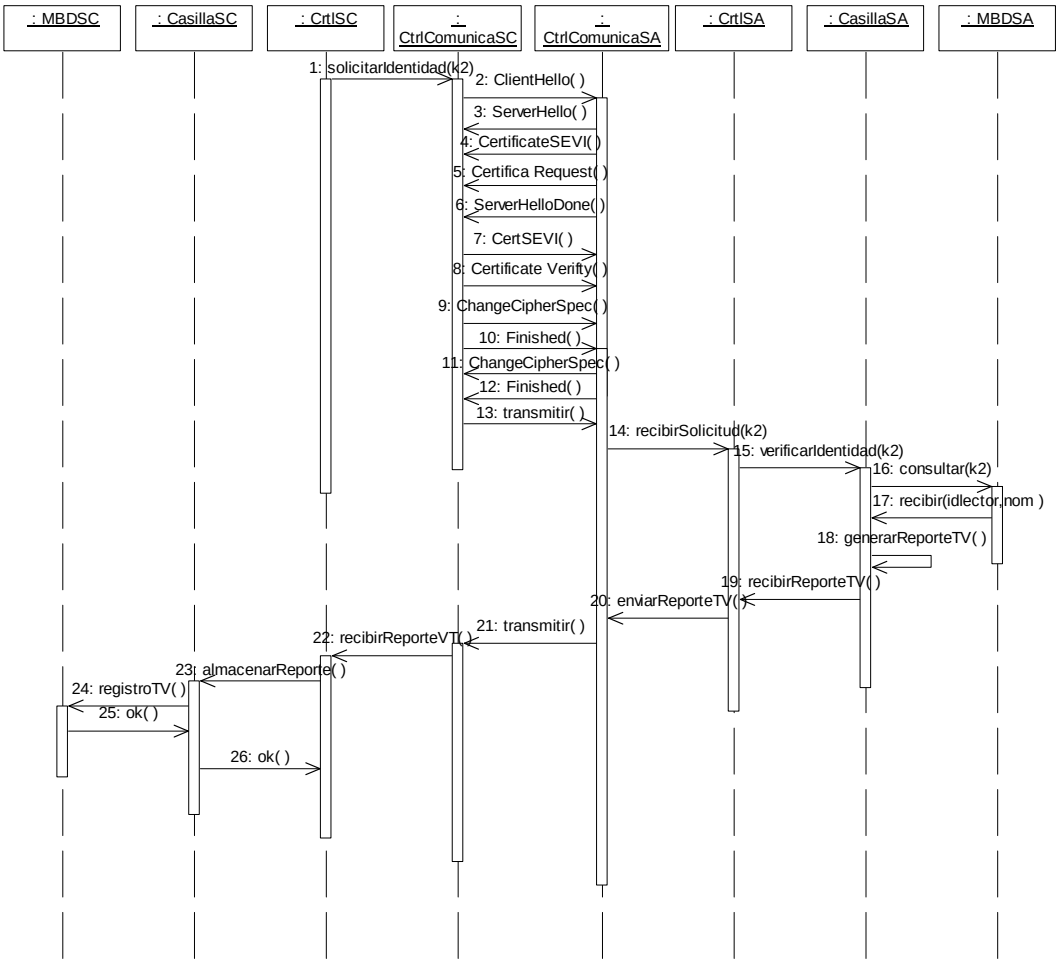


Fig. 5.21 Diagrama de secuencia generación de resultados.

Caso de uso auditar distrito

En este caso de uso los Representantes conforman el grupo que vigila el proceso electoral (consejeros electorales, representantes de cada partido político, presidente, secretario y escrutadores de la mesa de escrutinio, administradores y supervisores del sistema). El diagrama de clases refinado para este caso de uso se muestra en la Fig. 5.22.

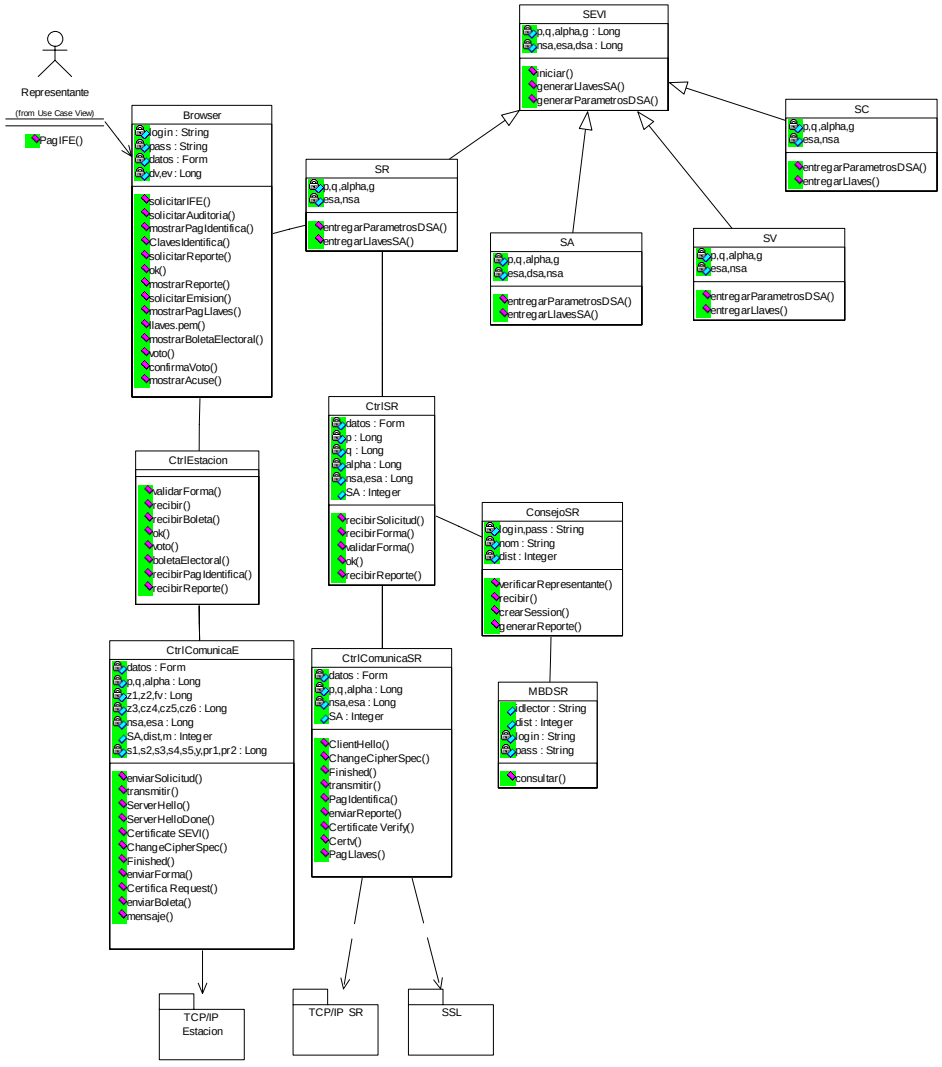


Fig. 5.22Diagrama de Clases Refinado Auditar Distrito.

El administrador es el encargado de generar las claves de identificación (login y pass) para cada Representante, permitiéndoles con eso la generación de reportes en las distintas etapas del proceso electoral

La clase consejo es la encargada de validar la identidad del representante y de generarle el reporte solicitado. La Fig. 5.23 presenta el diagrama de secuencia de la auditoria distrital.

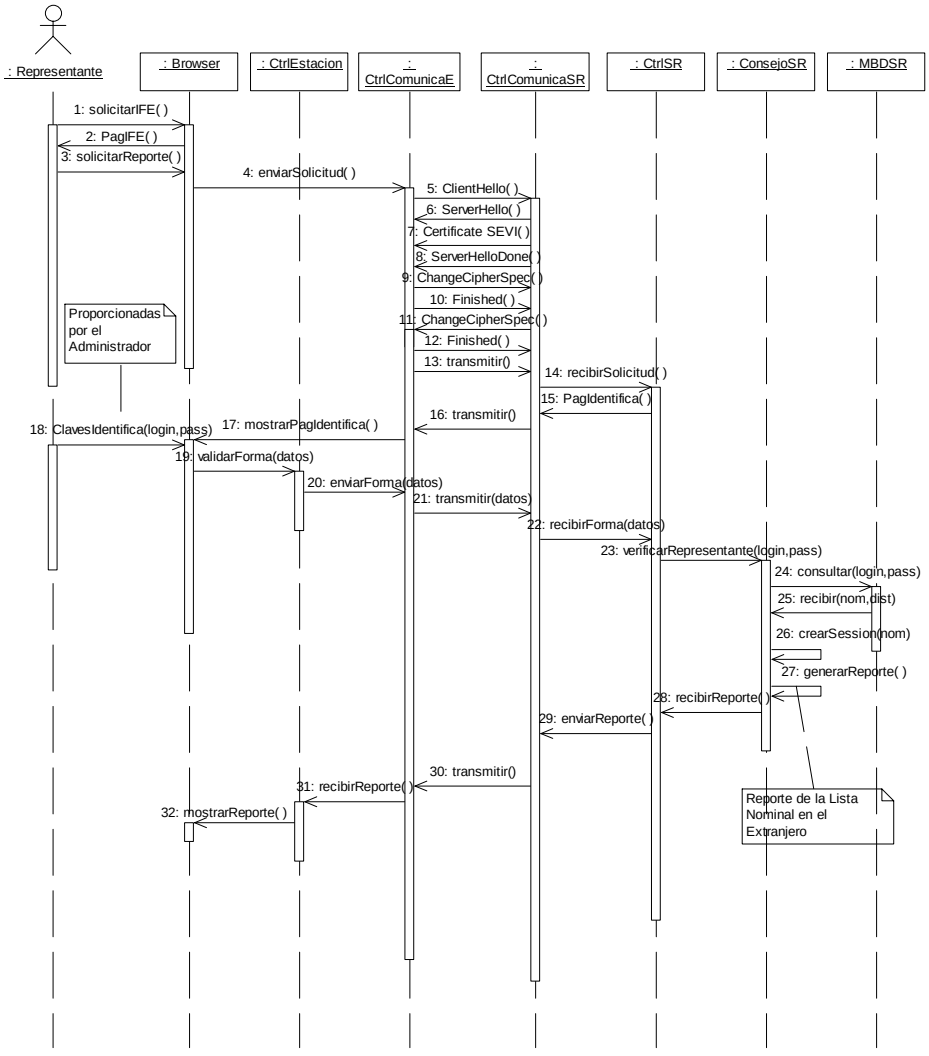


Fig. 5.23 Diagrama de secuencia auditar distrito.

Según lo indicado en la ley electoral artículos 281 y 282, el servicio de auditoria estará abierto a los representantes una vez cerrado el periodo de registro y sólo se les podrá generar reportes de la lista nominal, sin dar derecho a modificaciones (altas o bajas).

Para el periodo de votación y conteo, se seguirá lo establecido en el artículo 294. Los reportes informarán el resultado final de la votación, número de votos válidos, votos nulos y votos inválidos por distrito electoral y entidad federativa. Podrán solicitarse también la identidad de los votantes tramposos.

Caso de uso auditar voto

El diagrama de clases refinado se muestra en la Fig. 5.24. Cuando el ciudadano emite su voto, el sistema le proporciona un acuse de recibo, con la indicación de que su voto ya fue depositado. Para asegurar que fue contabilizado, se genera un reporte con el identificador del ciudadano y su acuse de recibo, sin mostrar el valor de su voto.

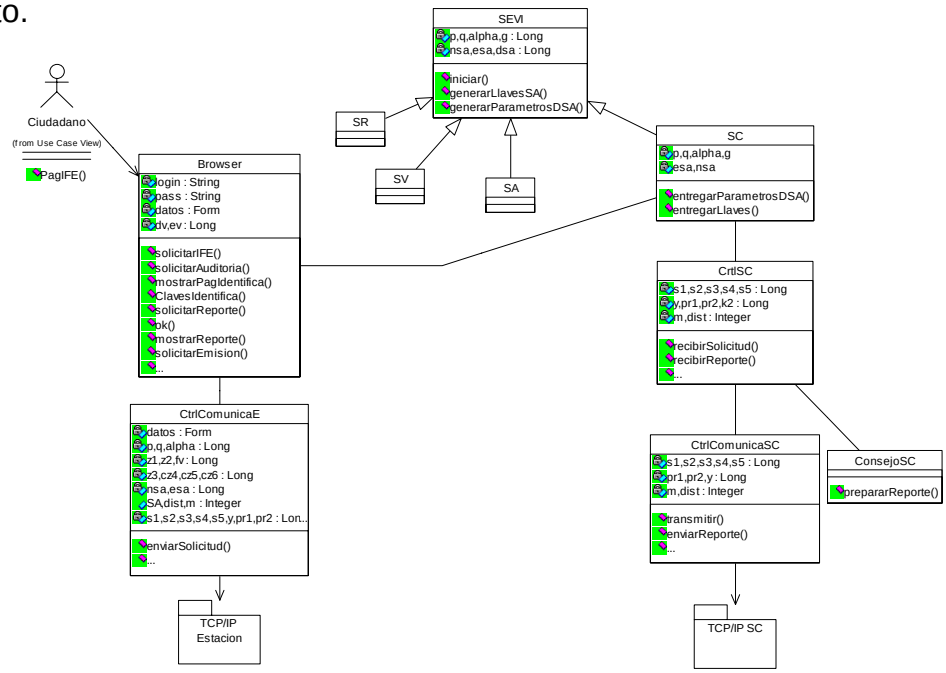


Fig. 5.24 Diagrama de clases refinado auditar voto.

No se requiere de ninguna identificación ya que es de dominio público. El diagrama de secuencia se muestra en la Fig. 5.25.

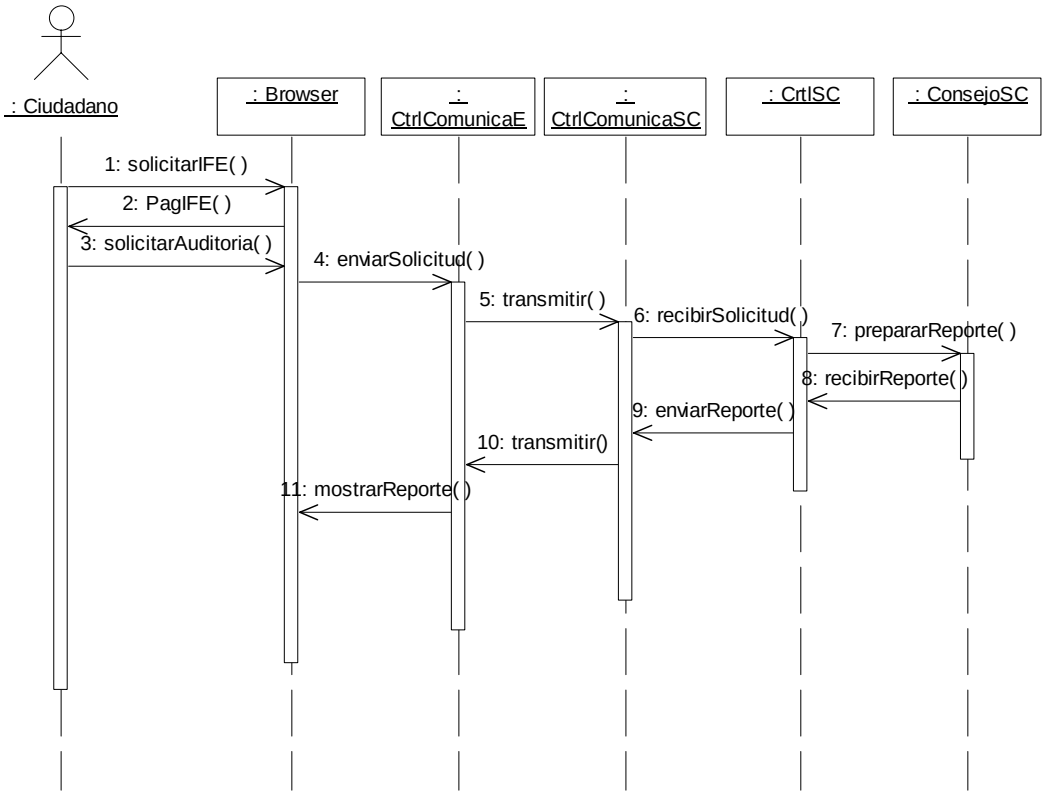


Fig. 5.25 Diagrama de secuencia auditar voto.

Caso de uso inicia sistema

Este caso de uso es interno en SEVI. Su función es iniciar las variables de seguridad usadas por los servidores al implementar el protocolo de seguridad basado en Lin-Hwang-Chang.

Básicamente es la creación de los parámetros de la firma digital DSA (*p,q,alpha*) y de las llaves pública y privada del SA. Las Fig. 5.26 y 5.27 nos muestran el diagrama de clases refinado y de secuencia para este caso de uso.

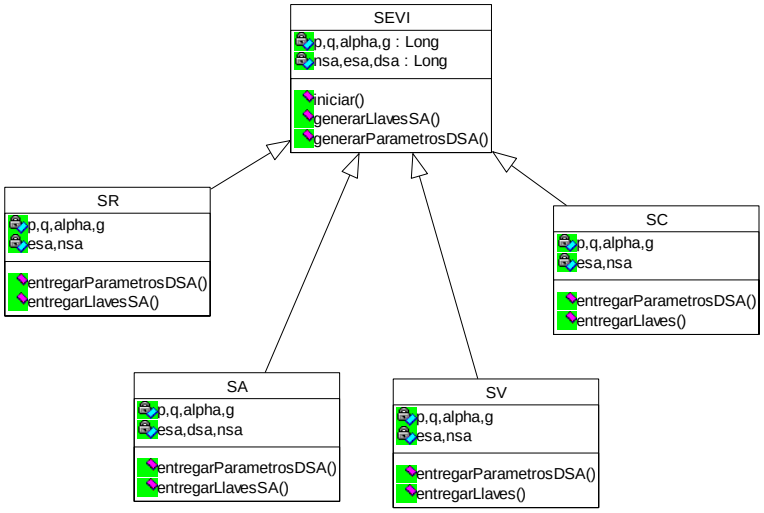


Fig. 5.26 Diagrama de clases refinado inicia sistema.

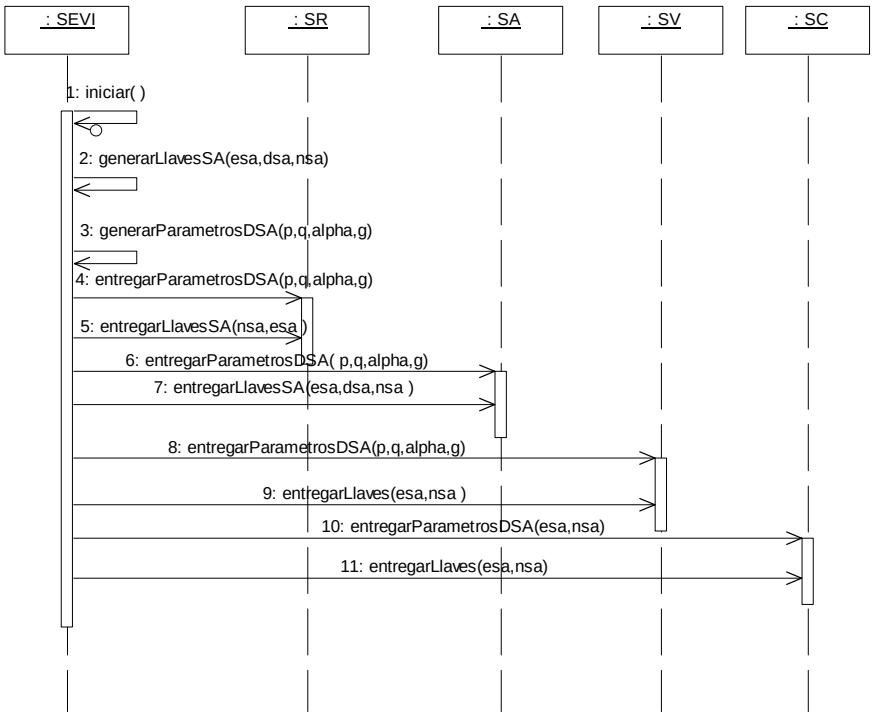


Fig. 5.27 Diagrama de secuencia inicia sistema.

Capítulo 6

Modelo de Implementación y Pruebas SEVI

En el modelo de implementación se modela la configuración de los elementos de procesado en tiempo de ejecución y de los componentes, procesos y objetos de software que viven en ellos. Cuando se diseña un sistema, hay que considerar tanto su dimensión lógica como su dimensión física. En la parte lógica aparecen cosas como clases, interfaces, interacciones, etc. En la parte física se encuentran los componentes que representan los empaquetamientos físicos de esos elementos lógicos y los nodos que representan el hardware sobre el que se despliegan y ejecutan esos componentes.

Un diagrama de despliegue son uno de los dos tipos de diagramas que aparecen cuando se modelan los aspectos físicos de los sistemas orientados a objetos, muestra la configuración de nodos que participan en la ejecución y de los componentes que residen en ellos.

Antes de presentar el diagrama de despliegue de SEVI, debemos recordar que es un sistema distribuido, los servidores de los que se compone se encuentran separados y son independientes uno del otro, la comunicación entre ellos se hace a través de Internet, así como la

comunicación con las terminales (PC) que solicitan los servicios. En la Fig. 6.1 se muestra el modelo cliente/servidor de SEVI, el cual se compone de cuatro servidores que apoyan las tareas más importantes del proceso electoral (Registro, Autenticación, Votación y Conteo).

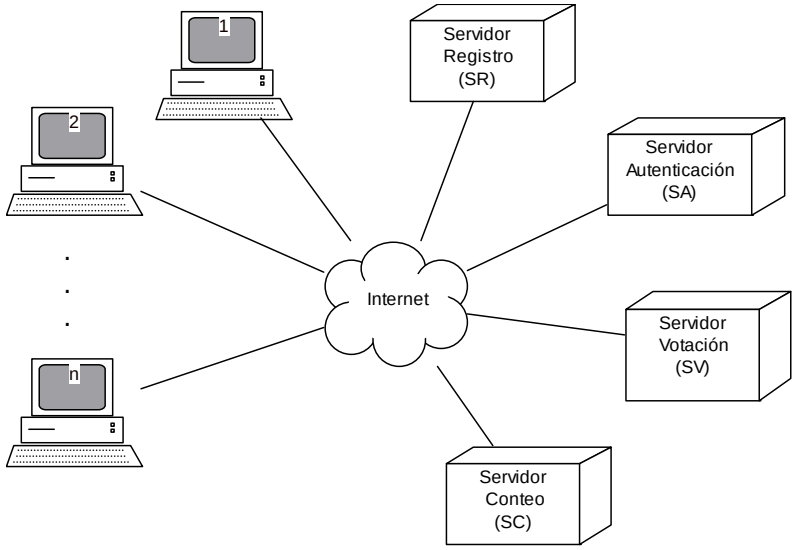


Fig. 6.1 Modelo cliente/servidor SEVI

Pero no todos los nodos se comunican entre sí, eso depende del periodo en el que se encuentre el proceso electoral.

La Fig. 6.2 muestra el diagrama de despliegue de los servidores que conforman al sistema SEVI, donde pueden apreciarse todas las conexiones que son posibles en todos los periodos en los que se divide el proceso electoral.

La terminal que representa la máquina cliente usada por el ciudadano o el representante mantiene comunicación con todos los servidores, esto es por que en el caso de uso auditoria, se le permite a los representantes (según el periodo en que se encuentre el proceso electoral) la generación de reportes, como ejemplo del uso de cada servidor sería para el SR la solicitud de las listas nominales, para el SA la lista de votantes, para el SV la impresión del acuse de recibo, para el

SC la generación de resultados y la visualización del número de votos emitidos (válidos y nulos).

La conexión entre el SV y el SC se refiere al paso de las boletas electorales. La solicitud de la identidad del votante tramposo justifica la conexión entre el SA y el SC.

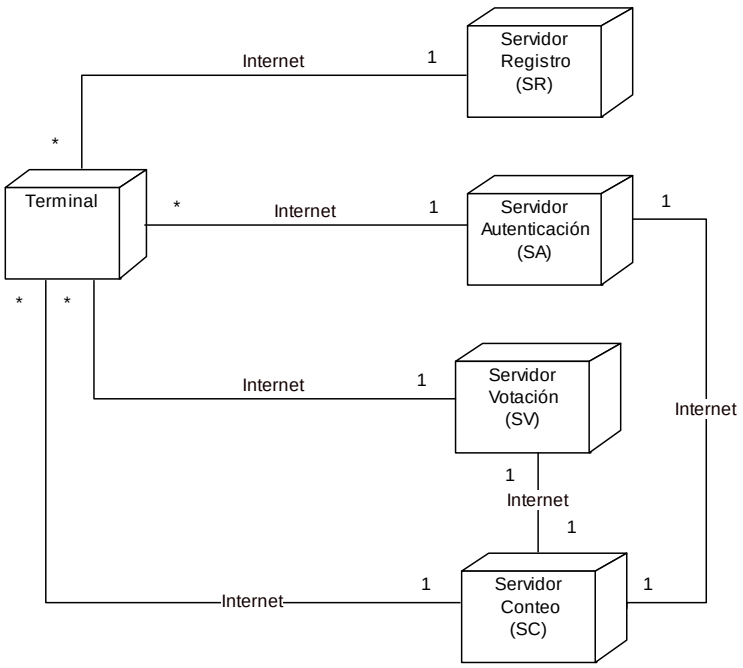


Fig. 6.2 Conexión entre los servidores y la terminal en SEVI

Los servidores deben ser independientes respecto a la ejecución de sus procesos, la dependencia que puede haber entre ellos es respecto a los pasos en serie del proceso electoral, como lo es que el servidor de autenticación no puede ponerse en marcha hasta que el servidor de registro culmina el periodo de registro, el servidor de votación recibe votos una vez que el servidor de autenticación confirmó la identidad del ciudadano, el servidor de conteo ofrece servicio una vez que haya terminado el periodo de votación.

Todos los servidores tienen las mismas características, la Fig. 6.3 muestra los paquetes y las librerías que se utilizan, la especificación de cada paquete es el siguiente:

- GMP 4.2.1: Librería criptográfica, usada para la programación del protocolo de seguridad basado en Lin-Hwang-Chang.
- PHP 5.1: Lenguaje de programación.
- OpenSSL: Librería criptográfica usada para el establecimiento de la conexión segura.
- Oracle 9i: manejador de bases de datos.
- SSL: protocolo de comunicación con conexión segura.
- TCP/IP: protocolo de comunicación por Internet.

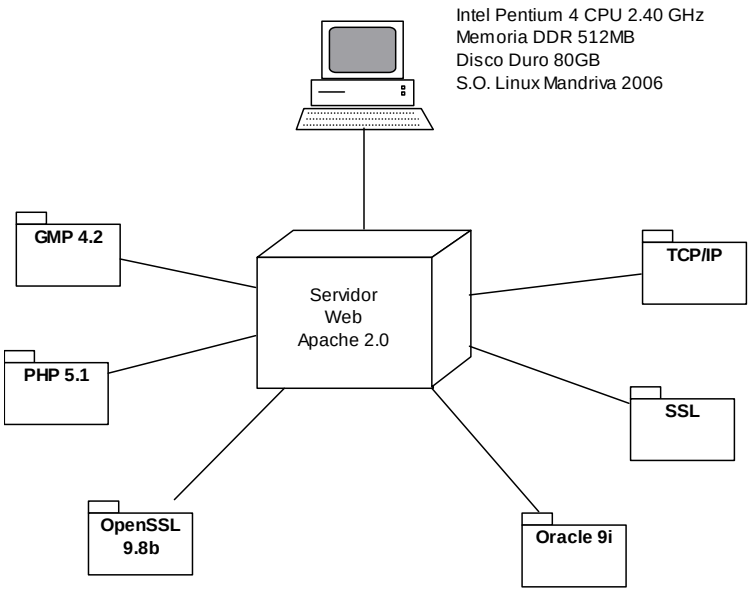


Fig. 6.3 Composición de los servidores que forman SEVI.

6.1 Implementación de los casos de uso

6.1.1 Registro

Este servicio permite a los ciudadanos mexicanos radicados en el extranjero, solicitar su registro en la Lista Nominal de Electores en el Extranjero (LNEE).

El Instituto Federal Electoral debe autorizar el acceso a su base de datos (BDIFE), en donde se encuentra la información del Padrón Electoral y de la Lista Nominal de Electores para consulta de los datos a fin de realizar las comparaciones necesarias para la validación y aceptación del ciudadano. El diseño de las bases de datos se realizó para $70x10^6$ votantes.

La comparación se hace con los datos personales (nombre completo, edad, sexo, firma), datos electorales (clave de elector, año de registro, sección y estado) y la imagen de la fotografía del ciudadano.

La Fig. 6.4 presenta el diagrama de componentes del caso de uso registro. La página principal es index.html y contiene: las ligas de las páginas candidato_1.htm a candidato_n.htm que son de divulgación; la liga a la consulta que va a explicarse en el caso de uso consultar estado del trámite y por último la liga de la página de registro.

Al solicitar el registro se establece una conexión segura a través de SSL con el certificado digital de SEVI para que la página de registro sea presentada en el navegador. El ciudadano ingresa los datos requeridos, indica el término de la captura y antes de transmitir la información se realiza la verificación de los datos con validación.js [26].

Cubierta la validación, la información se transmite y se procesa en Registro, desde las clases ModuloIFE y Seguridad Servidor, con la ayuda de las librerías oci8 para la conexión con Oracle 9i [27,28], gmp.c para la criptografía [29,30] y openssl [31] para la generación de certificados digitales. Por último, se responde al ciudadano informando

que se recibió correctamente su información y se le solicita consultar posteriormente el estado de su trámite en confirma.htm. La Fig. 6.5 muestra la página principal de SEVI.

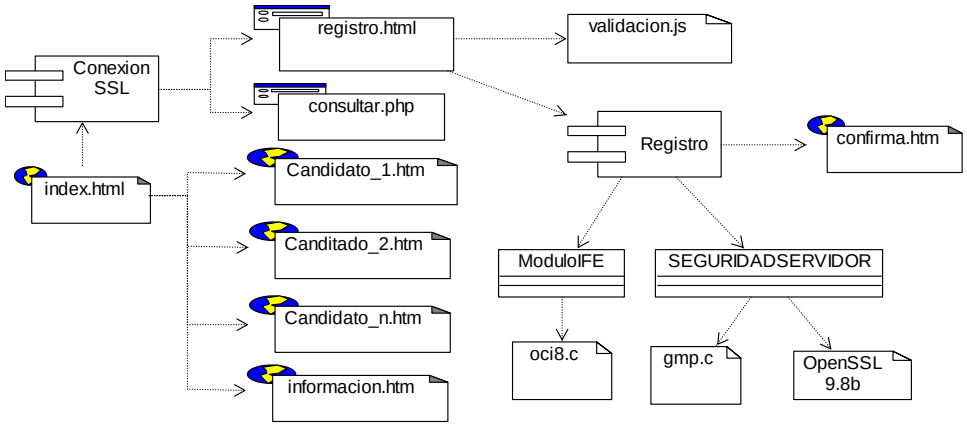


Fig. 6.4 Diagrama de componentes registro

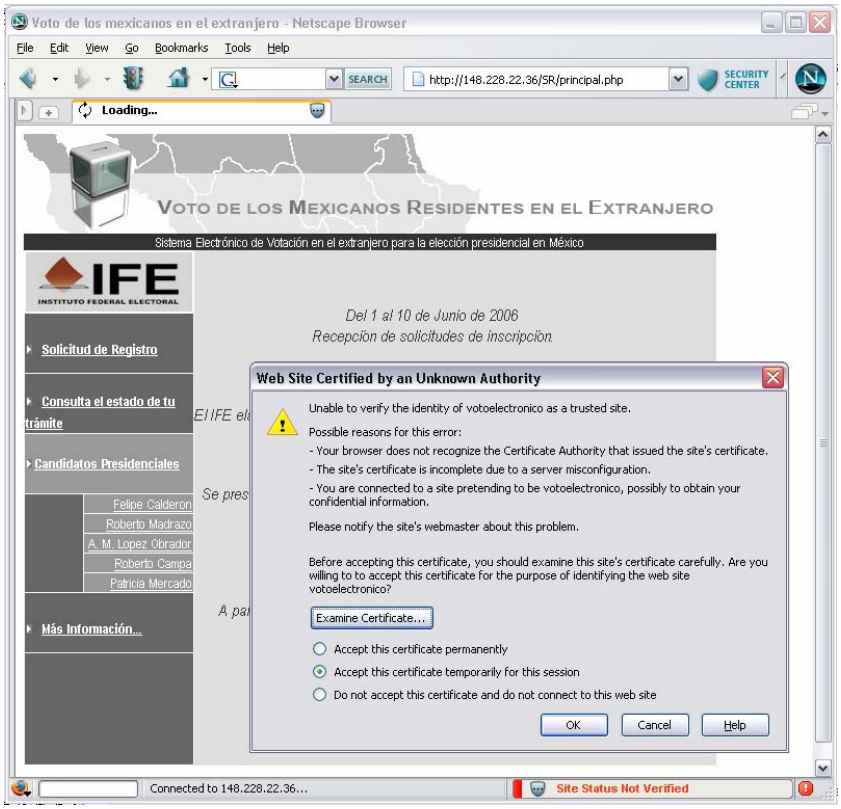


Fig. 6.5 Página principal registro SEVI

El Certificado Digital fue creado con la aplicación OpenSSL 9.8b, con las siguientes características:

Algoritmo de Llave Pública: PKCS#1 RSA ENCRYPTION

Firma Digital: SHA-1 WITH RSA ENCRYPTION

Nombre del Certificado: SEVIFE

Nombre de la Entidad Certificadora: CA_ServIFE

Algoritmo de Cifrado: AES-256bits

La página de Registro se encuentra dividida en cinco secciones, debido a que la ley electoral indica que el ciudadano debe proporcionar:

- Datos de su Credencial de Elector (Personales y Electorales)
- Su Domicilio en el Extranjero
- Su Firma (clave de Identificación)
- Copia digital de su credencial de elector y de su constancia de domicilio
- Aceptar la baja temporal de su registro en el Listado Nominal Electoral

La Fig. 6.6 muestra la página de registro.

Sección A: Datos de tu credencial de Elector, aquí se solicita toda la información presente en la credencial de elector. Se le pide al ciudadano coloque sus datos tal y como están en la credencial, además para su ayuda y ubicación, del lado derecho se colocó una credencial de elector indicando la posición de cada dato sobre la misma.

Sección B: Datos de tu Domicilio en el Extranjero, se le pide al ciudadano ingrese la dirección donde radica actualmente, con el fin de distinguir cuantas solicitudes se reciben de cada país.

Sección C: Datos de Ingreso Seguro, aunque la identificación del ciudadano sobre el Padrón Electoral Nacional se hace a través de la

clave de elector, se solicita ingrese el login y el password, con la restricción de que deben de ser únicas, así, se dificultará a la persona que desee tomar credenciales de elector que no son suyas y quiera registrarlas.

Sección D: Comprobantes, bajo la votación en el extranjero con la modalidad postal, solicitan la copia de la credencial de elector y de la constancia de domicilio, la primera es para corroborar la identidad del ciudadano y la segunda es para confirmar la dirección para que pueda ser enviada la boleta electoral al lugar correcto, en esta sección por tanto se solicitan las copias digitalizadas de las mismas.

Sección E: Condiciones del Servicio, es importante que en cada registro que se haga, el usuario confirme bajo que condiciones le ofrecen el servicio, así en SEVI, se informa al ciudadano como va a ser manipulada su información y se solicita confirmar su autorización.

Descripción de autorizar registro

Método que se encarga de verificar que los datos contengan información válida. Primero confirma que el ciudadano solicitante no esté dado de baja en el Listado Nominal Electoral, ya que significaría que fue aceptado en la Lista Nominal Electoral en el Extranjero.

La siguiente comprobación se refiere a la identidad del ciudadano a través de la comparación de los datos proporcionados en la Sección A de la página de registro, contra los datos del registro encontrado en el Listado Nominal Electoral en la BDIFE, si coinciden en su totalidad, entonces se procede al registro en la Lista Nominal de Electores en el Extranjero y a la baja temporal en la Lista Nominal Electoral.

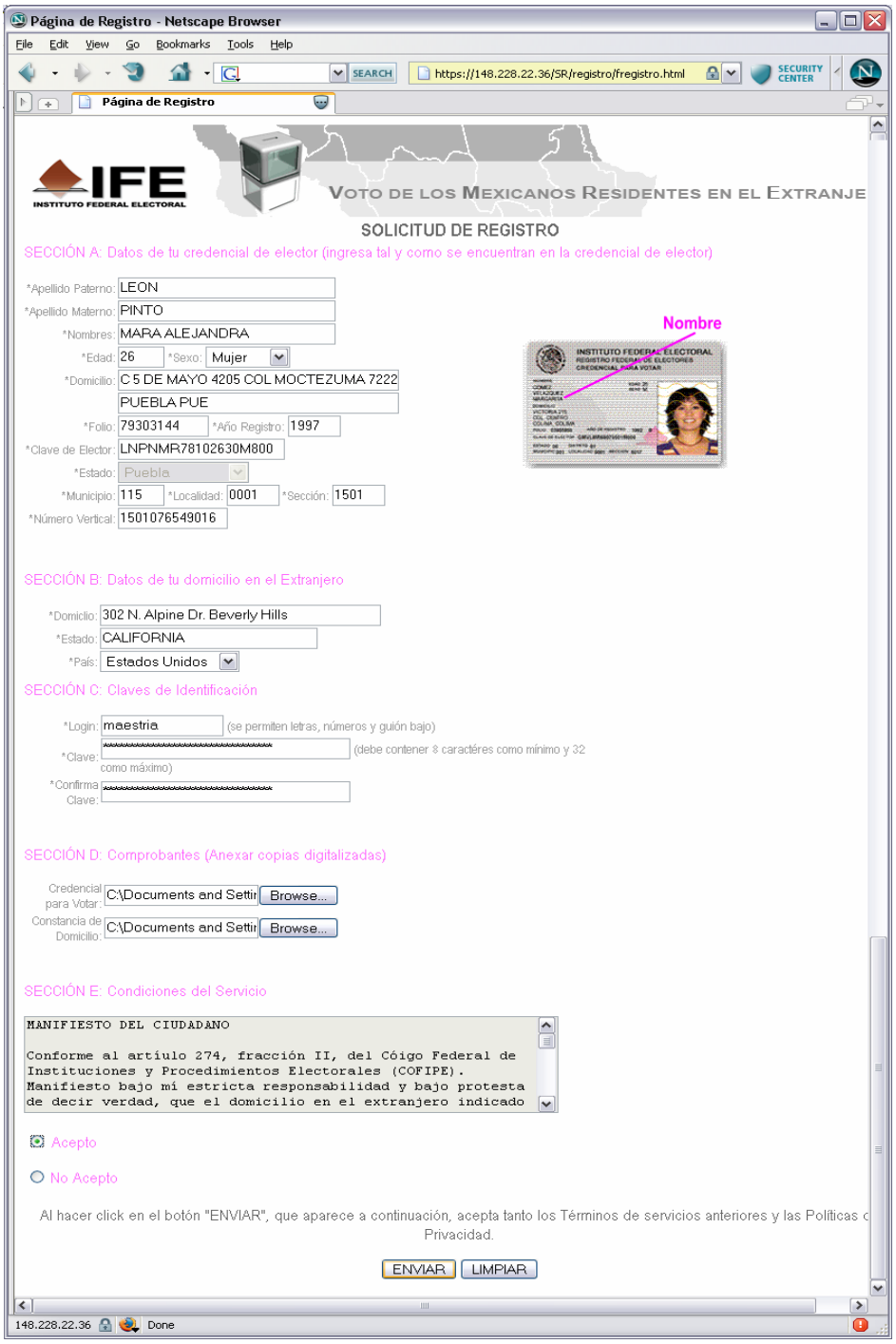


Fig. 6.6 Página de registro SEVI.

6.1.2 Consultar el estado del trámite

Este caso de uso es muy importante, a través de él, los ciudadanos pueden verificar si fueron aceptados o rechazados para poder votar por Internet. En el primer caso, el ciudadano debe descargar el certificado digital y sus llaves pública y privada que se le solicitarán en la fase de votación para su identificación ante el SA. En el segundo caso, SEVI le informará al ciudadano la causa del rechazo a su solicitud de registro. La Fig. 6.7 nos muestra el diagrama de componentes para este caso de uso. La página principal es la misma que la de registro, la liga que accede a la consulta es consultar.php y se presenta después de establecer un canal seguro con SSL.

Consiste en una forma que solicita la identificación del ciudadano con el ingreso de su login y password, una vez validada la forma con validación.js, la información se transmite al servidor de registro, se procesa en Consultar usando principalmente la clase ModuloIFE.

La verificación de las claves de identificación del ciudadano requiere la consulta a la base de datos de registro con ayuda de la librería oci8.c. Si el ciudadano es aceptado, prepara la dirección donde se encuentra almacenado el certificado digital del ciudadano para su descarga. Si el ciudadano fue rechazado, responde con la página de acuerdo a la razón de su rechazo.

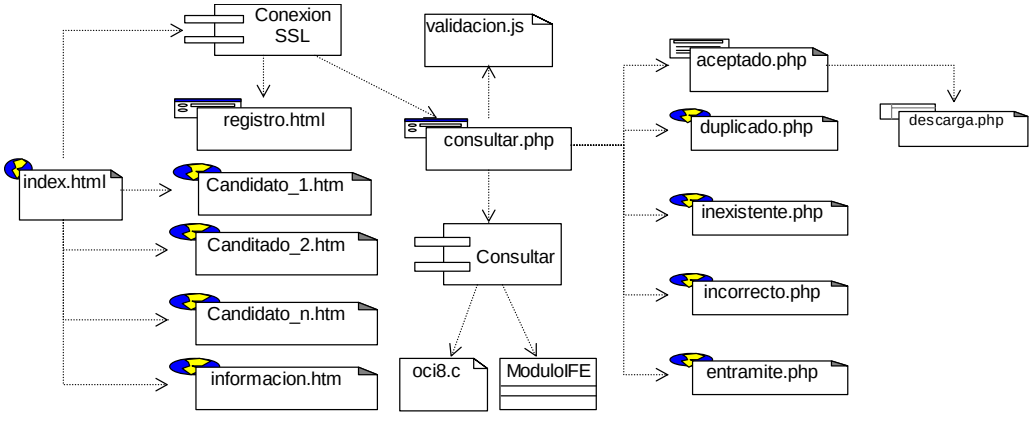


Fig. 6.7 Diagrama de componentes consulta estado del trámite.

Las Fig. 6.8 y 6.9 nos muestran las páginas de consulta y el caso de aceptación del ciudadano.

Fig. 6.8 Ventana de identificación para consultar el estado del trámite.

Fig. 6.9 Página de aceptación de registro para el usuario.

6.1.3 Votación

Para emitir el voto, se sigue el protocolo de seguridad basado en Lin-Hwang-Chang, en este caso de uso sólo se cubren las dos primeras fases del protocolo: Autenticación y Votación.

El ciudadano debe solicitar su voto a través de la página principal. La opción de emisión sólo estará disponible en el periodo indicado en la ley electoral.

El diagrama de componentes se muestra en la Fig. 6.10.

Antes de presentar la boleta electoral electrónica, el ciudadano debe ingresar sus claves de identificación (login y password) y su certificado digital. La información se transmite a través del canal seguro y se procesa en Autenticar, la clase Casilla valida el registro del ciudadano para convertirlo en votante y le responde con la forma contenida en el archivo procesa.php, que tiene como función solicitarle sus llaves pública y privada y hacer el cálculo para la solicitud de las firmas a ciegas al SA.

El SA recibe el mensaje, la clase Seguridad Servidor se encarga de autenticar al votante con el certificado y la firma digital recibidas. Si todo está en orden, firma a ciegas y envía la boleta electoral en boleta.php para la emisión del voto.

El votante recibe la boleta electoral y procesa en Seguridad Estación las firmas para obtener su acreditación ante el SV. Emite su voto lo firma, para enviarlo al SV y ser procesado en Votar quien recibe la boleta electoral para verificarla con la clase Seguridad Servidor, si es correcta se almacena el voto desde la clase Casilla y se responde al votante con un acuse de recibo en acuse.php.

Las Fig. 6.11 y 6.12 muestran la boleta electoral y el acuse de recibo para un votante.

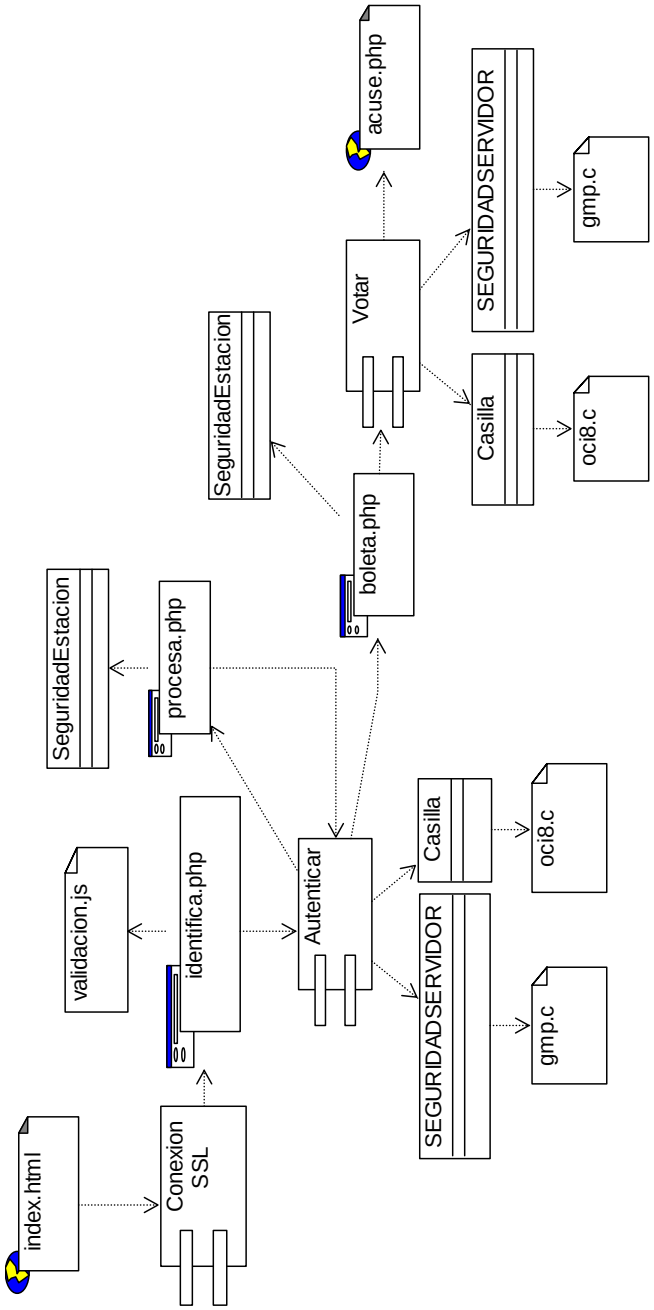


Fig. 6.10 Diagrama de componentes votación

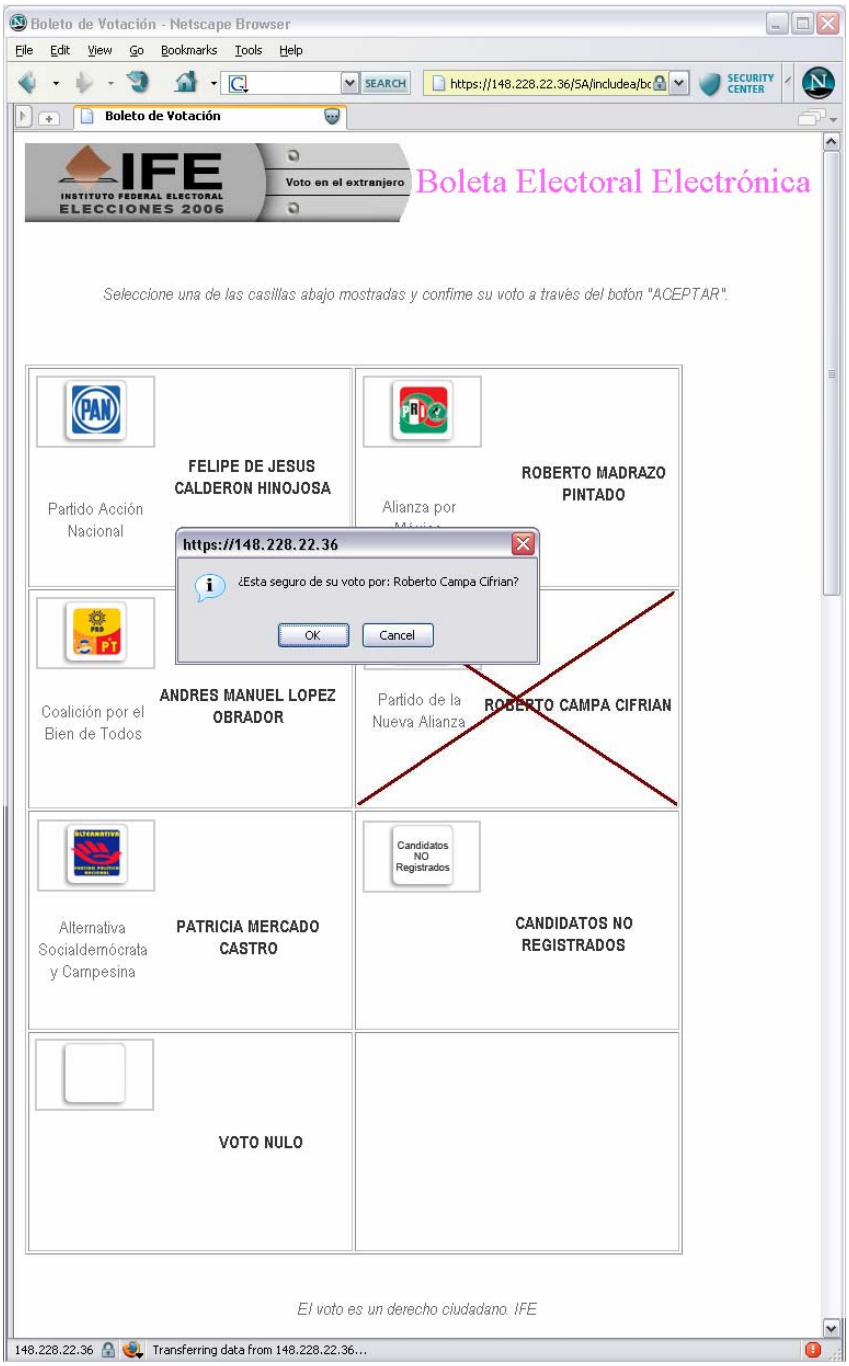


Fig. 6.11 Boleta electoral SEVI

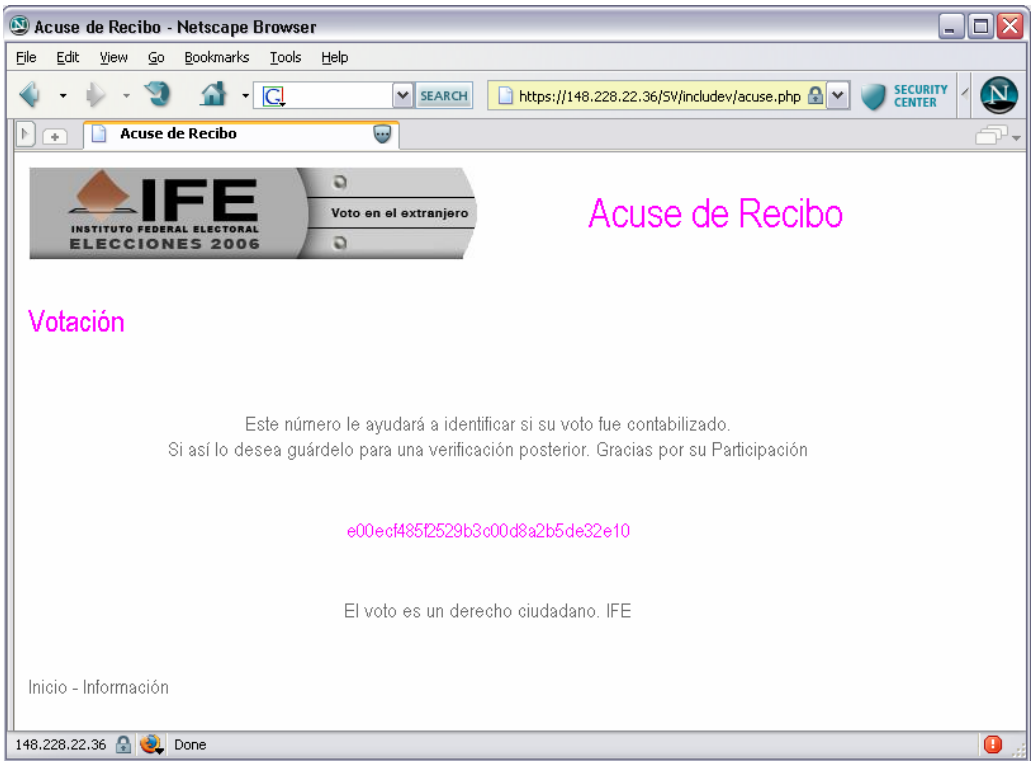


Fig. 6.12 Acuse de recibo para el Ciudadano SEVI

6.1.4 Generación de resultados

En este caso de uso, se cubre la fase de conteo del protocolo de seguridad para votaciones electrónicas, el diagrama de componentes se ilustra en el Fig. 6.13 y consiste en el paso de las boletas electorales del SV al SC. La transmisión es iniciada por el mismo servidor al cumplirse el día y la hora establecida para el escrutinio de los votos en la ley electoral. Se reciben las boletas y se procesan en Contar con la ayuda de la clase Seguridad Servidor. Al término del conteo, si se detectaran votantes tramposos, se hace la solicitud a Autenticar para identificar a esos votantes.

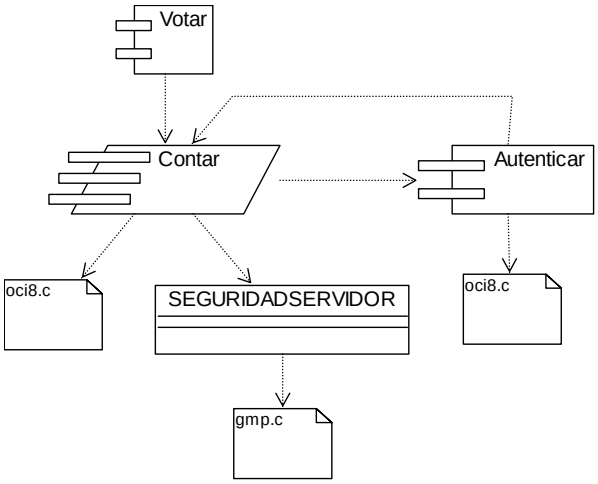


Fig. 6.13 Diagrama de componentes generación de resultados

Como no se tiene una vista al público de este servicio, las Fig. 6.14 y 6.15, nos muestran el contenido de las tablas donde se almacena la información. En la primera figura se ilustran las boletas electorales divididas en las firmas que las forman, el valor del voto y el distrito electoral a donde pertenece el voto. En la figura siguiente, se encuentra la tabla donde se almacenan los resultados por distrito electoral.

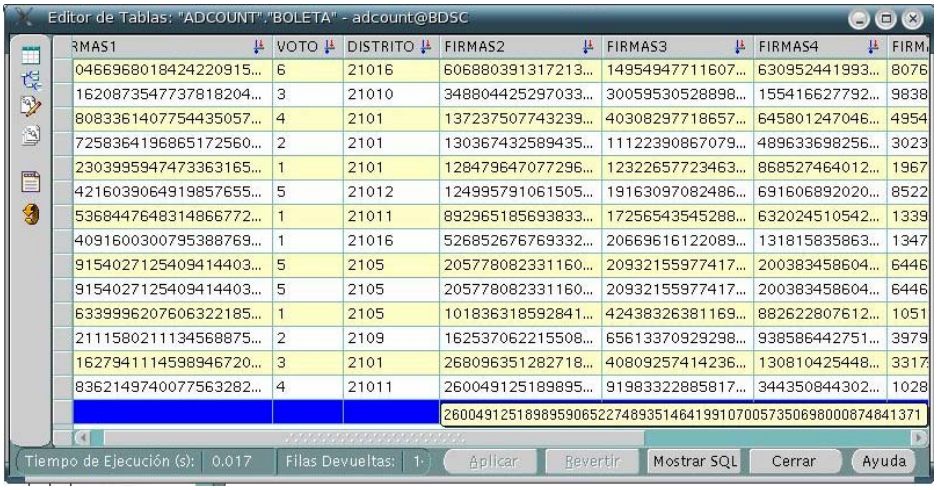


Fig. 6.14 Consulta BDSC de las boletas electorales

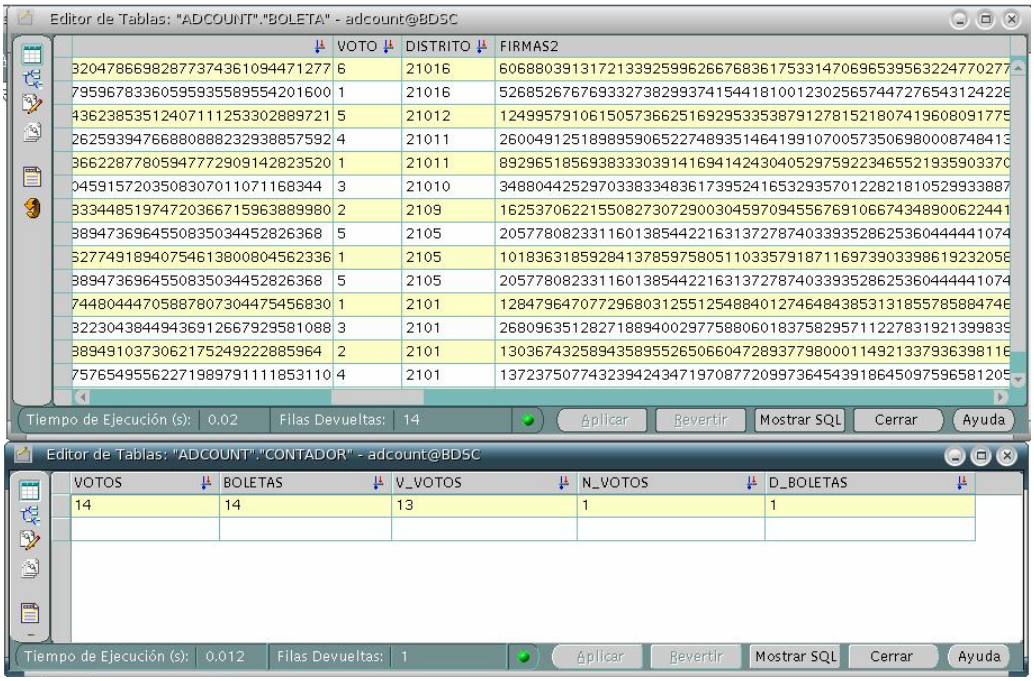


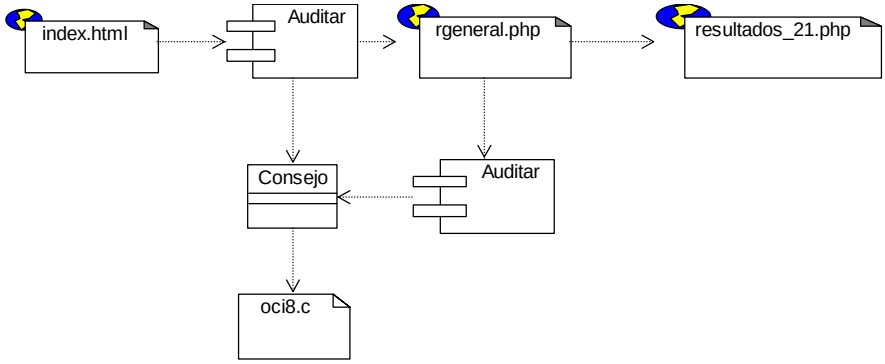
Fig. 6.15 Consulta BDSC de los resultados al término de la jornada electoral

6.1.5 Auditar distrito

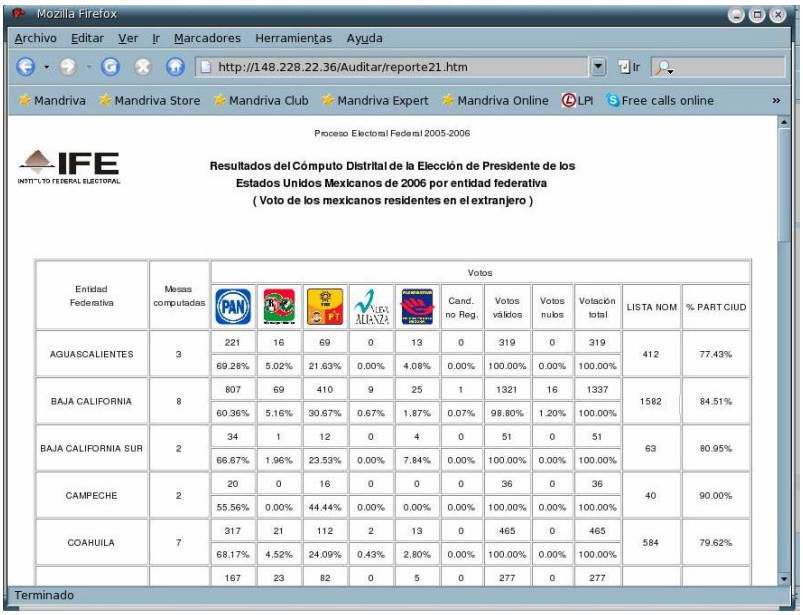
La función de este caso de uso, es informar al representante (consejero electoral, representante de partido político, presidente, secretario y escrutadores de la mesa de escrutinio, supervisores del sistema y administradores), por medio de reportes solicitados a las bases de datos, según el periodo en el que se encuentre el proceso electoral.

En el caso del periodo de verificación de la Lista Nominal de Electores en el Extranjero (LNEE), se solicita la identificación del solicitante, si es válida entonces se abre la ventana de diálogo para la descarga del archivo en modo texto.

En caso de la verificación de la jornada electoral, las páginas expuestas al público son la de los resultados generales de todas las entidades federativas y los resultados para cada entidad federativa. La Fig. 6.16 muestra el Diagrama de componentes para este caso. Las Figuras 6.17 y 6.18 ilustran las páginas de resultados generales y de la entidad federativa número 21 que es el estado de Puebla.



6.16 Diagrama de Componentes auditar distrito de los resultados de la votación.



Entidad Federativa	Mesas computadas	Votos											
		PAN		PT	Alianza		Cand. no Reg.	Votos válidos	Votos nulos	Votación total	LISTA NOM	% PART CIUD
AGUASCALIENTES	3	221	16	69	0	13	0	319	0	319	412	77.43%
		69.28%	5.02%	21.63%	0.00%	4.08%	0.00%	100.00%	0.00%	100.00%		
BAJA CALIFORNIA	8	807	69	410	9	25	1	1321	16	1337	1582	84.51%
		60.36%	5.16%	30.67%	0.67%	1.87%	0.07%	98.80%	1.20%	100.00%		
BAJA CALIFORNIA SUR	2	34	1	12	0	4	0	51	0	51	63	80.95%
		66.67%	1.96%	23.53%	0.00%	7.84%	0.00%	100.00%	0.00%	100.00%		
CAMPECHE	2	20	0	16	0	0	0	36	0	36	40	90.00%
		55.56%	0.00%	44.44%	0.00%	0.00%	0.00%	100.00%	0.00%	100.00%		
COAHUILA	7	317	21	112	2	13	0	465	0	465	584	79.62%
		68.17%	4.52%	24.09%	0.43%	2.80%	0.00%	100.00%	0.00%	100.00%		
		167	23	82	0	5	0	277	0	277		

Fig. 6.17 Resultados generales de la jornada electoral SEVI

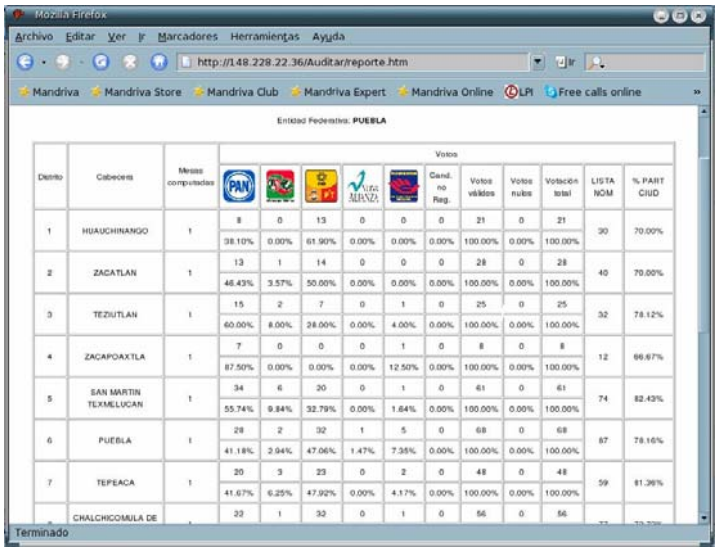


Fig. 6.18 Resultados del estado de Puebla de la jornada electoral SEVI

Un reporte completo sólo es posible desde la consulta de la base de datos directamente en el servidor, consulta realizada sólo por los supervisores o administradores del sistema. Lo anterior se debe a lo dicho en la ley electoral (Artículo 294 del COFIPE), que se informará por escrito el resultado del computo distrital a los Consejeros Distritales y a los Partidos Políticos.

6.1.5 Auditar voto

Para la auditoria de los votos por parte de los ciudadanos votantes, no se requiere identificación ya que será información expuesta al público. Se hará desde la página principal la cual contendrá la liga verifica_voto.php. Esta página mostrará el listado de los acuses de recibo entregados a cada votante al término de la emisión de su voto. Bastará con que el votante busque su acuse de recibo para comprobar que su voto fue contabilizado. La Fig. 6.19 muestra la página de verificación y la Fig. 20 la página de acuse del Ciudadano votante.

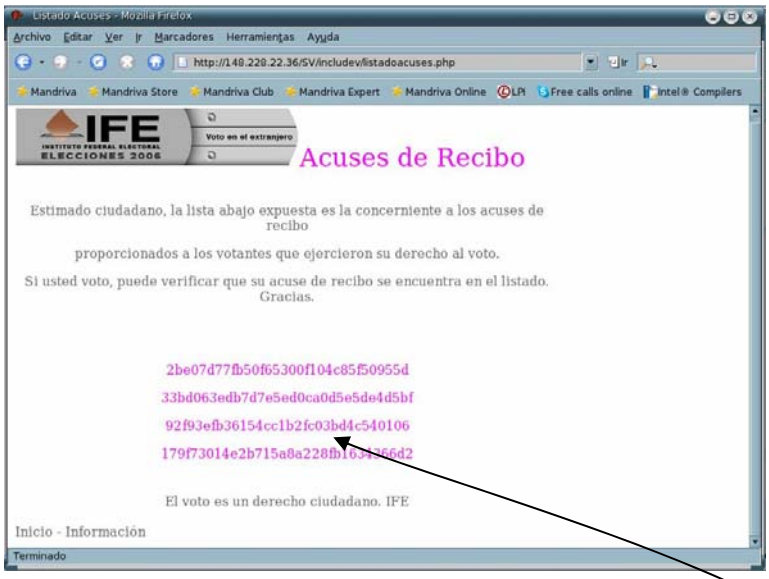


Fig. 6.20 Página de verificación del voto.

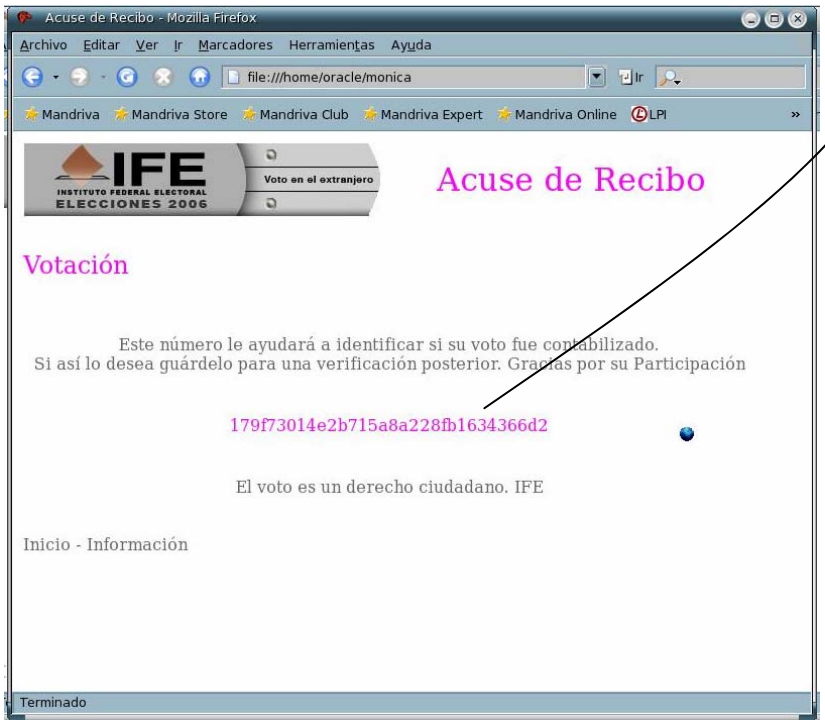


Fig. 6.21 Acuse de recibo del votante.

6.2 Modelo de pruebas

SEVI fue diseñado para tolerar grandes cantidades de información. En la fase de registro se manipularon 3.5 millones de registros para la simulación de la Lista Nominal Electoral.

Se registraron desde distintas computadoras (PC) 123 registros en un periodo de tiempo de una semana obteniendo lo siguiente:

- 4 registros duplicados,
- 21 registros con errores de captura,
- 2 registros inexistentes,
- 96 registros válidos y autorizados para votar.

En la emisión del voto, se abrió el periodo de votación la siguiente semana a la del registro, consiguiendo lo siguiente:

- 85 Ciudadanos autenticados,
- 82 votos emitidos,
- 14 votos duplicados,
- 3 votos no recibidos,
- 11 Ciudadanos que se registraron pero no votaron.

Los reportes de los resultados son generados por única ocasión al término del conteo y almacenados en un archivo html, mismo que se encuentra disponible para cualquier persona que desee observar la información por Internet.

Los comentarios de los Ciudadanos que utilizaron el sistema fueron:

1. Solicitar correo para entregar las claves de identificación olvidadas por los Ciudadanos.

2. Indicar el tamaño de la contraseña para saber el máximo de seguridad.
3. Aumentar el tamaño de caracteres para la dirección en el extranjero.
4. Aumentar número de países en la dirección del extranjero.
5. Verificación de los rangos de validación para las secciones y los municipios.
6. Sugerir cuenta electrónica de contacto por parte de SEVI a los Ciudadano votantes.
7. La página de acuse de recibido no presentada en por lo menos tres emisiones del voto.
8. Confusión en el ingreso del certificado digital y el archivo que contiene las llaves pública y privada.

Cabe señalar que las pruebas mostradas se refieren a un primer bosquejo de la funcionalidad de SEVI. No se analizan tiempos de ejecución ni costo de las operaciones criptográficas realizadas.

La razón es por la falta de infraestructura para probar el sistema, ya que sólo se cuenta con una máquina que contiene los cuatro servidores de los que se compone SEVI y la base de datos que simula la Lista Nominal Electoral del IFE.

Capítulo 7

Conclusiones

El presente trabajo presenta el desarrollo del Sistema Electrónico de Votación por Internet (SEVI), correspondiente a la propuesta de automatización para el proceso electoral por correo postal certificado para la emisión del voto de los ciudadanos mexicanos radicados en el extranjero.

Para lograr la automatización, primero se realizó un análisis de la ley electoral en el Libro Sexto del Código Federal de Instituciones y Procedimientos Electorales (COFIPE), artículos 273 al 300.

Debido a que el sistema de software es un sistema electrónico de votación por Internet, se investigaron los distintos tipos de votación electrónica, tomando como base para la seguridad aplicada en SEVI la implementada en el Sistema Electrónico para Elecciones Seguras (SELES), a través del protocolo de seguridad basado en Lin-Hwang-Chang, debido a que cubre el proceso de votación en tres fases: Autenticación, Votación y Conteo y es capaz de detectar votos duplicados así como la identidad del votante tramposo.

La metodología utilizada para el desarrollo del sistema fue el Proceso Unificado de Desarrollo de Software, construyendo con el Lenguaje Unificado de Modelado (UML) los modelos de Casos de Uso, Análisis, Diseño e Implementación.

SEVI consta de cuatro servidores que cubren los servicios fundamentales de Registro, Autenticación, Votación, Conteo y Auditoria.

Dado que SEVI es una propuesta de automatización para un proceso electoral en el Instituto Federal Electoral, se respeto la arquitectura de los servidores del instituto, como lo es el uso del sistema operativo Linux y del manejador de base de datos Oracle en su versión 9i.

La activación de los servicios ofrecidos por cada servidor depende de los periodos establecidos en el Libro Sexto del COFIPE, es decir el Servidor de Registro podrá estar abierto para el registro del 1ro de octubre del año previo a la elección al 15 de enero del año electoral, el Servidor de Autenticación y Votación estarán disponibles del 15 de abril al 1ro de julio del año electoral y por último el Servidor de Conteo comenzará sus funciones a las diecisiete horas del día 2 de julio del año electoral.

La auditoria al proceso puede realizarse también respetando el periodo señalado por la ley, sin embargo también se permite la generación de reportes en todo el proceso electoral por parte de los administradores y supervisores del sistema.

Los protocolos de seguridad aplicados en SEVI son el Protocolo para Transmisión Segura SSL (Secure Sockets Layer) y el Protocolo de votación electrónica basado en Lin-Hwang-Chang. Para el proceso de votación los algoritmos criptográficos clave son las firmas a ciegas basadas en RSA y las firmas digitales con DSA, más el uso de certificados digitales y la generación de llaves públicas y privadas para cada votante.

7.1 Trabajo futuro

SEVI opera según lo establecido en la ley electoral indicada en el Libro Sexto del COFIPE, esa razón justifica el hecho de solicitar una imagen digitalizada de la constancia de domicilio, sin embargo, bajo la modalidad del voto electrónico, es suficiente con la indicación del estado o país de residencia a fin de lograr estadísticas de las solicitudes y del lugar donde son generadas, aún así se solicita la dirección en el extranjero completa, una mejora al sistema sería contar con un subsistema que nos permita verificar la validez de la dirección proporcionada por el ciudadano.

Siguiendo con las imágenes, SEVI solicita también la copia digitalizada de la credencial de elector, con el fin de cotejar la fotografía de la credencial de elector con la almacenada en la base de datos del IFE, ésta comparación no se realiza debido a no tener una imagen del ciudadano en la base de datos que simula a la del IFE. Sin embargo si se tuviera, para hacer la comparación de manera automática, un trabajo futuro sería aplicar el reconocimiento de patrones a las imágenes.

En este trabajo se construyeron los modelos de caso de uso, análisis, diseño e implementación. En el modelo de pruebas sólo se presenta una primera aproximación de la funcionalidad del sistema, quedando como trabajo futuro una prueba piloto sobre un proceso de votación real.

SEVI fue desarrollado bajo la arquitectura cliente/servidor, sin embargo no fue posible la puesta en marcha de los servidores de manera separada, pues se necesitaban como mínimo cuatro máquinas y cuatro direcciones IP estáticas y sólo se contaba con dos máquinas y dos direcciones IP (una estática y otra dinámica). La implementación de los cuatro servidores en sus propias máquinas servidor queda también como trabajo futuro.

Apéndice A

Libro Sexto del COFIPE

La ley electoral para el periodo electoral 2005-2006 se reformó con el fin de permitir a los ciudadanos mexicanos radicados en el extranjero emitir su voto a través del correo postal certificado.

Las reformas de algunos artículos y la adición de otros autorizan e indican los pasos a seguir para esta modalidad del voto y se exponen en este apartado tal cual se presentan en el Código Federal de Instituciones y Procedimientos Electorales (COFIPE).

SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CÓDIGO FEDERAL DE INSTITUCIONES Y PROCEDIMIENTOS ELECTORALES

ARTÍCULO PRIMERO.- Se **reforman** los Artículos 1, 9 y el inciso c) del párrafo 1 del Artículo 250; y se adiciona un nuevo inciso al párrafo 1 del Artículo 250, para que el actual inciso d) pase a ser e) del Código Federal de Instituciones y Procedimientos Electorales, para quedar como sigue:

Artículo 1

1. Las disposiciones de este Código son de orden público y de observancia general en el territorio nacional y para los ciudadanos

mexicanos que ejerzan su derecho al sufragio en territorio extranjero en la elección para Presidente de los Estados Unidos Mexicanos.

2. ...

Artículo 9

1. El ejercicio del Poder Ejecutivo se deposita en un solo individuo que se denomina Presidente de los Estados Unidos Mexicanos electo cada seis años por mayoría relativa y voto directo de los ciudadanos mexicanos.

...

Artículo 250.

1. **...**

a) **...**

b) **...**

c) Se sumarán los resultados obtenidos según los dos incisos anteriores;

d) El cómputo distrital de la elección de Presidente de los Estados Unidos Mexicanos, será el resultado de sumar a los resultados obtenidos según el inciso anterior, los consignados en el acta distrital de cómputo de los votos emitidos en el extranjero, a que se refieren los Artículos 294 y 295 de este Código. El resultado así obtenido se asentará en el acta correspondiente a esta elección, y

e) Se harán constar en el acta circunstanciada de la sesión los resultados del cómputo y los incidentes que ocurrieren durante la misma.

...

ARTÍCULO SEGUNDO.- Se **reforma** la denominación del Libro Sexto y se le adicionan los Artículos 273 al 300 todos relativos al Código Federal de Instituciones y Procedimientos Electorales, para quedar como sigue:

LIBRO SEXTO
DEL VOTO DE LOS MEXICANOS RESIDENTES EN EL EXTRANJERO
TÍTULO ÚNICO

Artículo 273
1. Los ciudadanos que residan en el extranjero podrán ejercer su derecho al voto exclusivamente para la elección de Presidente de los Estados Unidos Mexicanos.

Artículo 274
1. Para el ejercicio del voto los ciudadanos que residan en el extranjero, además de los que fija el Artículo 34 de la Constitución y los señalados en el párrafo 1 del Artículo 6 de este Código, deberán cumplir los siguientes requisitos:
I. Solicitar a la Dirección Ejecutiva del Registro Federal de Electores, por escrito, con firma autógrafa o, en su caso, huella digital, en el formato aprobado por el Consejo General, su inscripción en el listado nominal de electores residentes en el extranjero;
II. Manifestar, bajo su más estricta responsabilidad y bajo protesta de decir verdad, el domicilio en el extranjero al que se le hará llegar, en su caso, la boleta electoral, y
III. Los demás establecidos en el presente Libro.

Artículo 275
1. Los ciudadanos mexicanos que cumplan los requisitos señalados enviarán la solicitud a que se refiere el inciso I del párrafo 1 del Artículo anterior entre el 1o. de octubre del año previo, y hasta el 15 de enero del año de la elección presidencial.
2. La solicitud será enviada a la Dirección Ejecutiva del Registro Federal de Electores, por correo certificado, acompañada de los siguientes documentos:

a) Fotocopia legible del anverso y reverso de su credencial para votar con fotografía; el elector deberá firmar la fotocopia o, en su caso, colocar su huella digital, y
b) Documento en el que conste el domicilio que manifiesta tener en el extranjero.
3. Para efectos de verificación del cumplimiento del plazo de envío señalado en el párrafo 1 de este Artículo, se tomará como elemento de prueba la fecha de expedición de la solicitud de inscripción que el servicio postal de que se trate estampe en el sobre de envío.
4. A ninguna solicitud enviada por el ciudadano después del 15 de enero del año de la elección, o que sea recibida por el Instituto después del 15 de febrero del mismo año, se le dará trámite. En estos casos, la Dirección Ejecutiva del Registro Federal de Electores enviará al interesado, por correo certificado, aviso de no inscripción por extemporaneidad.
5. El ciudadano interesado podrá consultar al Instituto, por vía telefónica o electrónica, su inscripción.

Artículo 276
1. La solicitud de inscripción en el listado nominal de electores tendrá efectos legales de notificación al Instituto de la decisión del ciudadano de votar en el extranjero en la elección para Presidente de los Estados Unidos Mexicanos. Para tal efecto el respectivo formato contendrá la siguiente leyenda: “Manifiesto, bajo protesta de decir verdad, que por residir en el extranjero:
a) Expreso mi decisión de votar en el país en que resido y no en territorio mexicano;
b) Solicito votar por correo en la próxima elección para Presidente de los Estados Unidos Mexicanos;
c) Autorizo al Instituto Federal Electoral, verificado el cumplimiento de los requisitos legales, para ser inscrito en la lista nominal de electores residentes en el extranjero, y darme de baja, temporalmente, de la lista correspondiente a la sección electoral que aparece en mi credencial para votar;

d) Solicito que me sea enviada a mi domicilio en el extranjero la boleta electoral, y
e) Autorizo al Instituto Federal Electoral para que, concluido el proceso electoral, me reinscriba en la lista nominal de electores correspondiente a la sección electoral que aparece en mi credencial para votar".

Artículo 277
1. Las listas nominales de electores residentes en el extranjero son las relaciones elaboradas por la Dirección Ejecutiva del Registro Federal de Electores que contienen el nombre de las personas incluidas en el Padrón Electoral que cuentan con su credencial para votar, que residen en el extranjero y que solicitan su inscripción en dichas listas.
2. Las listas nominales de electores residentes en el extranjero serán de carácter temporal y se utilizarán, exclusivamente, para los fines establecidos en este Libro.
3. Las listas nominales de electores residentes en el extranjero no tendrán impresa la fotografía de los ciudadanos en ellas incluidos.
4. El Consejo General podrá ordenar medidas de verificación adicionales a las previstas en el presente Libro a fin de garantizar la veracidad de las listas nominales de electores residentes en el extranjero.
5. Serán aplicables, en lo conducente, las normas contenidas en el Título Primero del Libro Cuarto de este Código.

Artículo 278
1. A partir del 1 de octubre del año previo al de la elección presidencial y hasta el 15 de enero del año de la elección, la Dirección Ejecutiva del Registro Federal de Electores pondrá a disposición de los interesados el formato de solicitud de inscripción en la lista nominal de electores residentes en el extranjero, en los sitios, en territorio nacional y en el extranjero, que acuerde la Junta General Ejecutiva, y a través de la página electrónica del Instituto.
2. Las sedes diplomáticas de México en el extranjero contarán con los formatos a que se refiere el párrafo anterior para que estén a

disposición de los ciudadanos mexicanos. El Instituto celebrará con la Secretaría de Relaciones Exteriores los acuerdos correspondientes.

Artículo 279

1. Las solicitudes de inscripción en la lista nominal de electores en el extranjero serán atendidas en el orden cronológico de su recepción, debiéndose llevar un registro de la fecha de las mismas.

2. Una vez verificado el cumplimiento de los requisitos, la Dirección Ejecutiva del Registro Federal de Electores procederá a la inscripción del solicitante en la lista nominal de electores residentes en el extranjero, dándolo de baja, temporalmente, de la lista nominal de electores correspondiente a la sección del domicilio asentado en su credencial para votar.

3. La Dirección Ejecutiva del Registro Federal de Electores conservará los documentos enviados y el sobre que los contiene hasta la conclusión del proceso electoral.

4. Concluido el proceso electoral, cesará la vigencia de las listas nominales de electores residentes en el extranjero. La Dirección Ejecutiva del Registro Federal de Electores procederá a reinscribir a los ciudadanos en ellas registrados, en la lista nominal de electores de la sección electoral que les corresponda por su domicilio en México.

5. Para fines de estadística y archivo, el Instituto conservará copia, en medios digitales, por un periodo de siete años, de las listas nominales de electores residentes en el extranjero.

Artículo 280

1. Concluido el plazo para la recepción de solicitudes de inscripción, la Dirección Ejecutiva del Registro Federal de Electores procederá a elaborar las listas nominales de electores residentes en el extranjero.

2. Las listas se elaborarán en dos modalidades:

a. Conforme al criterio de domicilio en el extranjero de los ciudadanos, ordenados alfabéticamente.

Estas listas serán utilizadas exclusivamente para efectos del envío de las boletas electorales a los ciudadanos inscritos.

b. Conforme al criterio de domicilio en México de los ciudadanos, por entidad federativa y distrito electoral, ordenados alfabéticamente. Estas listas serán utilizadas por el Instituto para efectos del escrutinio y cómputo de la votación.
3. En todo caso, el personal del Instituto y los partidos políticos están obligados a salvaguardar la confidencialidad de los datos personales contenidos en las listas nominales de electores residentes en el extranjero. La Junta General Ejecutiva dictará los acuerdos e instrumentará las medidas necesarias para tal efecto.
4. La Junta General Ejecutiva presentará al Consejo General un informe del número de electores en el extranjero, agrupados por país, estado o equivalente, y municipio o equivalente.

Artículo 281
1. Los partidos políticos, a través de sus representantes en la Comisión Nacional de Vigilancia, tendrán derecho a verificar las listas nominales de electores residentes en el extranjero, a que se refiere el inciso b del numeral 2 del Artículo anterior, a través de los medios electrónicos con que cuente la Dirección Ejecutiva del Registro Federal de Electores.
2. Las listas nominales de electores residentes en el extranjero no serán exhibidas fuera del territorio nacional.

Artículo 282
1. A más tardar el 15 de marzo del año de la elección presidencial, la Dirección Ejecutiva del Registro Federal de Electores pondrá a disposición de los partidos políticos las listas nominales de electores residentes en el extranjero.
2. Los partidos políticos podrán formular observaciones a dichas listas, señalando hechos y casos concretos e individualizados, hasta el 31 de marzo, inclusive.
3. De las observaciones realizadas por los partidos políticos se harán las modificaciones a que hubiere lugar y se informará al Consejo General y a la Comisión Nacional de Vigilancia a más tardar el 15 de mayo.

4. Los partidos políticos podrán impugnar ante el Tribunal Electoral el informe a que se refiere el párrafo anterior. La impugnación se sujetará a lo establecido en el párrafo 5 del Artículo 158 de este Código y en la ley de la materia.
5. Si no se impugna el informe o, en su caso, una vez que el Tribunal haya resuelto las impugnaciones, el Consejo General del Instituto sesionará para declarar que los listados nominales de electores residentes en el extranjero son válidos.

Artículo 283
1. La Junta General Ejecutiva deberá ordenar la impresión de las boletas electorales, de los sobres para su envío al Instituto, del instructivo para el elector y de los sobres en que el material electoral antes descrito será enviado, por correo certificado o mensajería, al ciudadano residente en el extranjero.
2. Para los efectos del párrafo anterior a más tardar el 31 de enero del año de la elección, el Consejo General del Instituto aprobará el formato de boleta electoral para la elección de Presidente de los Estados Unidos Mexicanos que será utilizada por los ciudadanos residentes en el extranjero, el instructivo para su uso, así como los formatos de las actas para escrutinio y cómputo y los demás documentos y materiales.
3. Serán aplicables, en lo conducente, respecto a la boleta electoral, las disposiciones del Artículo 205 de este Código. La boleta electoral que será utilizada en el extranjero contendrá la leyenda “Mexicano residente en el extranjero”.
4. El número de boletas electorales que serán impresas para el voto en el extranjero será igual al número de electores inscritos en las listas nominales correspondientes. El Consejo General determinará un número adicional de boletas electorales. Las boletas adicionales no utilizadas serán destruidas, antes del día de la jornada electoral, en presencia de representantes de los partidos políticos.

Artículo 284

1. La documentación y el material electoral a que se refiere el Artículo anterior estará a disposición de la Junta General Ejecutiva a más tardar el 15 de abril del año de la elección.

2. La Dirección Ejecutiva del Registro Federal de Electores pondrá a disposición de la Junta General Ejecutiva los sobres con el nombre y domicilio en el extranjero de cada uno de los ciudadanos inscritos en las listas nominales correspondientes, ordenados conforme a la modalidad establecida en el inciso a) del párrafo 2 del Artículo 280 de este Código.

3. La Junta General Ejecutiva realizará los actos necesarios para enviar, a cada ciudadano, por correo certificado con acuse de recibo, la boleta electoral, la documentación y demás material necesarios para el ejercicio del voto.

4. El envío de la documentación y material electoral antes señalados concluirá, a más tardar, el 20 de mayo del año de la elección.

Artículo 285

1. Recibida la boleta electoral el ciudadano deberá ejercer su derecho al voto, de manera libre, secreta y directa, marcando el recuadro que corresponda a su preferencia, en los términos del Artículo 218 de este Código.

2. El instructivo a que se refiere el párrafo 1 del Artículo 283 anterior, deberá incluir, al menos, el texto íntegro del Artículo 4 del presente Código.

Artículo 286

1. Una vez que el ciudadano haya votado, deberá doblar e introducir la boleta electoral en el sobre que le haya sido remitido, cerrándolo de forma que asegure el secreto del voto.

2. En el más breve plazo, el ciudadano deberá enviar el sobre que contiene la boleta electoral, por correo certificado, al Instituto Federal Electoral.

3. Para los efectos del párrafo anterior, los sobres para envío a México de la boleta electoral, tendrán impresa la clave de elector del ciudadano

remitente, así como el domicilio del Instituto que determine la Junta General Ejecutiva.

Artículo 287

1. La Junta General Ejecutiva dispondrá lo necesario para:

a) Recibir y registrar, señalando día, los sobres que contienen la boleta electoral, clasificándolos conforme a las listas nominales de electores que serán utilizadas para efectos del escrutinio y cómputo;

b) Colocar la leyenda "votó" al lado del nombre del elector en la lista nominal correspondiente; lo anterior podrá hacerse utilizando medios electrónicos, y

c) Resguardar los sobres recibidos y salvaguardar el secreto del voto.

Artículo 288

1. Serán considerados votos emitidos en el extranjero los que se reciban por el Instituto hasta veinticuatro horas antes del inicio de la jornada electoral.

2. Respecto de los sobres recibidos después del plazo antes señalado, se elaborará una relación de sus remitentes y acto seguido, sin abrir el sobre que contiene la boleta electoral, se procederá, en presencia de los representantes de los partidos políticos, a su destrucción.

3. El día de la jornada electoral el Secretario Ejecutivo rendirá al Consejo General del Instituto un informe previo sobre el número de votos emitidos por ciudadanos residentes en el extranjero, clasificado por país de residencia de los electores, así como de los sobres recibidos fuera de plazo a que se refiere el párrafo anterior.

Artículo 289

1. Con base en las listas nominales de electores residentes en el extranjero, conforme al criterio de su domicilio en territorio nacional, el Consejo General:

a) Determinará el número de mesas de escrutinio y cómputo que correspondan a cada distrito electoral uninominal. El número máximo de votos por mesa será de 1,500, y

b) Aprobará el método y los plazos para seleccionar y capacitar a los ciudadanos que actuarán como integrantes de las mesas de escrutinio y cómputo, aplicando en lo conducente lo establecido en el artículo 193 de este Código.
2. Las mesas de escrutinio y cómputo de la votación de los electores residentes en el extranjero se integrarán con un presidente, un secretario y dos escrutadores; habrá dos suplentes por mesa.
3. Las mesas antes señaladas tendrán como sede el local único, en el Distrito Federal, que determine la Junta General Ejecutiva.
4. Los partidos políticos designarán dos representantes por cada mesa y un representante general por cada veinte mesas, así como un representante general para el cómputo distrital de la votación emitida en el extranjero.
5. En caso de ausencia de los funcionarios titulares y suplentes de las mesas, la Junta General Ejecutiva determinará el procedimiento para la designación del personal del Instituto que los supla.
6. La Junta General Ejecutiva adoptará las medidas necesarias para asegurar la integración y funcionamiento de las mesas de escrutinio y cómputo.

Artículo 290
1. Las mesas de escrutinio y cómputo se instalarán a las 17 horas del día de la jornada electoral. A las 18 horas, iniciará el escrutinio y cómputo de la votación emitida en el extranjero.
2. El Consejo General podrá determinar el uso de medios electrónicos para el cómputo de los resultados y la elaboración de actas e informes relativos al voto de los electores residentes en el extranjero. En todo caso, los documentos así elaborados deberán contar con firma.

Artículo 291
1. Para el escrutinio y cómputo de los votos emitidos en el extranjero para la elección de Presidente de los Estados Unidos Mexicanos, se estará a lo siguiente:

a) El presidente de la mesa verificará que cuenta con el listado nominal de electores residentes en el extranjero que le corresponde, y sumará los que en dicho listado tienen marcada la palabra “votó”.
b) Acto seguido, los escrutadores procederán a contar los sobres que contienen las boletas electorales y verificarán que el resultado sea igual a la suma de electores marcados con la palabra “votó” que señala el inciso anterior.
c) Verificado lo anterior, el presidente de la mesa procederá a abrir el sobre y extraerá la boleta electoral, para, sin mayor trámite, depositarla en la urna; si abierto un sobre se constata que no contiene la boleta electoral, o contiene más de una boleta electoral, se considerará que el voto, o votos, son nulos y el hecho se consignará en el acta.
d) Los sobres que contengan las boletas serán depositados en un recipiente por separado para su posterior destrucción.
e) Una vez terminado lo anterior, dará inicio el escrutinio y cómputo, aplicándose, en lo conducente, las reglas establecidas en los incisos c) al f) del párrafo 1 del Artículo 229 y 233 de este Código.
f) Para determinar la validez o nulidad del voto, será aplicable lo establecido en el Artículo 230 de este Código y en el inciso c) de este párrafo.

Artículo 292
1. Las actas de escrutinio y cómputo de cada mesa serán agrupadas conforme al distrito electoral que corresponda.
2. El personal del Instituto designado previamente por la Junta General Ejecutiva, procederá, en presencia de los representantes generales de los partidos políticos, a realizar la suma de los resultados consignados en las actas de escrutinio y cómputo de las respectivas mesas para obtener el resultado de la votación emitida en el extranjero para la elección de Presidente de los Estados Unidos Mexicanos por distrito electoral uninominal, que será asentado en el acta de cómputo correspondiente a cada distrito electoral.

3. Las actas de cómputo distrital serán firmadas por el funcionario responsable y por el representante general de cada partido político designado para el efecto.
4. Los actos señalados en los párrafos anteriores de este Artículo serán realizados en presencia de los representantes generales de los partidos políticos para el cómputo distrital de la votación emitida en el extranjero.

Artículo 293
1. Concluido en su totalidad el escrutinio y cómputo de los votos emitidos en el extranjero, y después de que el presidente del Consejo General haya dado a conocer los resultados de los estudios a que se refiere el inciso k) del párrafo 1 del Artículo 83 de este Código, el Secretario Ejecutivo informará al Consejo General los resultados, por partido, de la votación emitida en el extranjero para Presidente de los Estados Unidos Mexicanos.
2. El Secretario Ejecutivo hará entrega a los integrantes del Consejo General del informe que contenga los resultados, por distrito electoral uninominal, de la votación recibida del extranjero y ordenará su inclusión, por distrito electoral y mesa de escrutinio y cómputo, en el sistema de resultados electorales preliminares.

Artículo 294
1. La Junta General Ejecutiva, por los medios que resulten idóneos, antes del miércoles siguiente al día de la jornada electoral, entregará, a cada uno de los Consejos Distritales, copia del acta de cómputo distrital a que se refiere el Artículo 292 de este Libro.
2. Los partidos políticos recibirán copia legible de todas las actas.
3. Las boletas electorales, los originales de las actas de escrutinio y cómputo de las mesas y del cómputo por distrito electoral uninominal, así como el informe circunstanciado que elabore la Junta General Ejecutiva, respecto de la votación emitida en el extranjero para la elección de Presidente de los Estados Unidos Mexicanos, serán integrados en un paquete electoral que será remitido, antes del

domingo siguiente al de la jornada electoral, a la Sala Superior del Tribunal Electoral, para los efectos legales conducentes.

Artículo 295

1. Realizados los actos a que se refiere el Artículo 250 de este Código, en cada uno de los Consejos Distritales el presidente del mismo informará a sus integrantes del resultado consignado en la copia del acta distrital de cómputo de los votos emitidos en el extranjero para Presidente de los Estados Unidos Mexicanos, para que sean sumados a los obtenidos del cómputo de los resultados de las casillas instaladas en el respectivo distrito.

2. El resultado de la suma señalada en el párrafo anterior se asentará en el acta a que se refiere el inciso d) del párrafo primero del Artículo 250 de este Código.

3. La copia certificada del acta distrital de cómputo de los votos emitidos en el extranjero para Presidente de los Estados Unidos Mexicanos en el distrito electoral respectivo, será integrada al expediente a que se refiere el inciso e) del párrafo 1 del Artículo 252 de este Código.

Artículo 296

1. Los partidos políticos nacionales y sus candidatos a cargos de elección popular no podrán realizar campaña electoral en el extranjero; en consecuencia, quedan prohibidas en el extranjero, en cualquier tiempo, las actividades, actos y propaganda electoral a que se refiere el Artículo 182 de este Código.

2. Durante el proceso electoral, en ningún caso y por ninguna circunstancia los partidos políticos utilizarán recursos provenientes de financiamiento público o privado, en cualquiera de sus modalidades, para financiar actividades ordinarias o de campaña en el extranjero.

Artículo 297

1. La violación a lo establecido en el Artículo anterior podrá ser denunciada, mediante queja presentada por escrito, debidamente fundada y motivada, aportando los medios de prueba, ante el Secretario

Ejecutivo del Instituto, por los representantes de los partidos políticos ante el Consejo General.

2. Para el desahogo de las quejas señaladas en el párrafo anterior, serán aplicables, en lo conducente, las disposiciones del Título Quinto, del Libro Quinto y los Artículos 49-A y 49-B de este Código.

3. Si de la investigación se concluye la existencia de la falta, las sanciones que se impondrán al partido político responsable serán las establecidas en el Artículo 269 de este Código, según la gravedad de la falta.

Artículo 298

1. Para el cumplimiento de las atribuciones y tareas que este Libro otorga al Instituto Federal Electoral, la Junta General Ejecutiva propondrá al Consejo General, en el año anterior al de la elección presidencial, la creación de las unidades administrativas que se requieran, indicando los recursos necesarios para cubrir sus tareas durante el proceso electoral.

Artículo 299

1. El costo de los servicios postales derivado de los envíos que por correo realice el Instituto a los ciudadanos residentes en el extranjero, será previsto en el presupuesto del propio Instituto.

Artículo 300

1. El Consejo General proveerá lo conducente para la adecuada aplicación de las normas contenidas en el presente Libro.

2. Son aplicables, en todo lo que no contravenga las normas del presente Libro, las demás disposiciones conducentes de este Código, la Ley General del Sistema de Medios de Impugnación en Materia Electoral y las demás leyes aplicables.

TRANSITORIOS

Artículo Primero.- Este Decreto entrará en vigor al día siguiente de su publicación en el **Diario Oficial de la Federación**.

Artículo Segundo.- Antes del mes de octubre de 2005, la Junta General Ejecutiva del Instituto Federal Electoral deberá formular y presentar, para su aprobación, al Consejo General, el programa que contenga las actividades relevantes y el proyecto de asignaciones presupuestarias en el ejercicio fiscal de 2005, las previsiones para el ejercicio fiscal de 2006 y, en su caso, la solicitud de ampliación del presupuesto 2005, para hacer posible el cumplimiento de las responsabilidades y tareas asignadas al Instituto por el Libro Sexto del Código Federal de Instituciones y Procedimientos Electorales que se reforma con el presente Decreto.

Artículo Tercero.- Se autoriza al Ejecutivo Federal, por conducto de la Secretaría de Hacienda y Crédito Público, para, en su caso, realizar las ampliaciones presupuestarias que resulten necesarias para proveer, en el ejercicio fiscal de 2005, al Instituto Federal Electoral, los recursos que solicite conforme al Artículo transitorio anterior. En su caso, esta autorización se entenderá otorgada al Ejecutivo Federal respecto de otros entes públicos que tengan participación directa en la aplicación de lo dispuesto por las adiciones al Libro Sexto que corresponden al presente Decreto.

Artículo Cuarto.- El Ejecutivo Federal, por conducto de la Secretaría de Hacienda y Crédito Público, informará a la Cámara de Diputados de las ampliaciones presupuestarias realizadas a favor del Instituto Federal Electoral en el ejercicio fiscal de 2005.

Artículo Quinto.- A partir de la entrada en vigor del presente Decreto, y hasta la conclusión del proceso electoral federal ordinario inmediato siguiente, se autoriza a la Junta General Ejecutiva del Instituto Federal Electoral para adjudicar en forma directa a los proveedores idóneos, tanto en México como en el extranjero, los contratos de adquisición de bienes, servicios y arrendamientos de inmuebles, cuando tal procedimiento sea necesario para garantizar el cumplimiento de los

plazos establecidos en las disposiciones adicionadas en el Libro Sexto que es materia de reforma del presente Decreto. Para tal efecto, los procedimientos para la adjudicación directa se sujetarán a lo establecido por el Artículo 41 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, sin que resulten aplicables los límites establecidos en el Presupuesto de Egresos de la Federación para los ejercicios fiscales de 2005 y 2006. La Junta General Ejecutiva informará al Consejo General de las resoluciones que adopte.

El Instituto Federal Electoral rendirá un informe de las adjudicaciones directas autorizadas conforme el presente Artículo al rendir las cuentas públicas correspondientes a los ejercicios fiscales de 2005 y 2006.

Artículo Sexto.- El Instituto Federal Electoral establecerá, en su caso, con el organismo público descentralizado denominado Servicio Postal Mexicano, y con los servicios postales del extranjero, los acuerdos necesarios para asegurar el eficiente, seguro y oportuno manejo, despacho, recepción y entrega de los documentos y materiales que se requieran para el ejercicio del derecho al voto de los mexicanos residentes en el extranjero.

Artículo Séptimo.- De ser necesario, con la participación del Instituto, el Titular del Poder Ejecutivo Federal por conducto de la Secretaría de Relaciones Exteriores, establecerá los acuerdos necesarios para coadyuvar al cumplimiento de lo establecido en el Artículo Transitorio anterior.

México, D.F., a 28 de junio de 2005.-
Sen. **Diego Fernández de Cevallos Ramos**, Presidente.-
Dip. **Manlio Fabio Beltrones Rivera**, Presidente.-
Sen. **Sara Isabel Castellanos Cortés**, Secretaria.-
Dip. **Graciela Larios Rivas**, Secretaria.- Rúbricas.

En cumplimiento de lo dispuesto por la fracción I del Artículo 89 de la Constitución Política de los Estados Unidos Mexicanos, y para su debida publicación y observancia, expido el presente Decreto en la Residencia del Poder Ejecutivo Federal, en la Ciudad de México, Distrito Federal, a los treinta días del mes de junio de dos mil cinco.-
Vicente Fox Quesada.- Rúbrica.-
El Secretario de Gobernación, **Carlos María Abascal Carranza**.- Rúbrica.

Apéndice B

Especificaciones SEVI

Como ya se mencionó en los capítulos anteriores, SEVI requiere de cuatro servidores, sus características y el software instalado es el siguiente:

Hardware

- Intel Pentium 4 CPU 2.40 GHz
- Memoria RAM DDR 512 MB
- Disco Duro 80 GB

Software

- Sistema Operativo Linux Mandriva 2006
- APACHE 2.0
- PHP 5.1.4
- GMP 4.2.1
- OPENSSL 9.8.b
- ORACLE 9i

B.1 Compilación de los paquetes instalados sobre Linux en cada servidor

B.1.1 OpenSSL 9.8.b

1. Código Fuente: openssl-0.9.8b.tar.gz
2. Directorio del fuente: /usr/src/openssl-9.8.b
3. Compilación:
    a. ./configure –prefix=/usr/local –openssldir=/usr/local/openssl
    b. # make
    c. # make test
    d. # make install
4. Creación del Certificado Digital para SEVI
    a. Generación del Certificado como Autoridad Certificadora
        - openssl genrsa –out ACSEV.pem –passout pass:servidorSEVI 2048
        - openssl req –new –x509 –out ACSEV.crt –days 365 –sha1 –config openssl.cnf –extensions v3_ca
            i. Key: **********
            ii. País: MX
            iii. Estado: Puebla
            iv. Ciudad: Puebla
            v. Organización: FCCBUAP
            vi. Departamento: Postgrado
            vii. Nombre Común: ACSEV

b. Generación del Certificado para el Servidor

- Openssl genrsa –out votoelectronico.pem –passout pass:servidorlinux 1024

c. Petición de Certificado a la Autoridad Certificadora

- Openssl req –new –out votoelectronico.csr –key votoelectronico.pem –sha1 –config openssl.cnf
  i. Key: **********
  ii. País: MX
  iii. Estado: Puebla
  iv. Ciudad: Puebla
  v. Organización: FCCPOSTGRADO
  vi. Departamento: GEN2004
  vii. Nombre Común: votoelectronico

d. Generación del Certificado de la llave pública del Servidor firmado por Autoridad Certificado.

- Openssl x509 –req –in votoelectronico.csr –CAkey ACSEV.pem –sha1 –days 365 –out votoelectronico.crt –signkey votoelectronico.pem –extfile openssl.cnf –extension v3_ca

Certificado: votoelectronico.csr

Llave privada: votoelectronico.pem

B.1.2 Apache 2.0

Mandriva 2006 contiene ya un paquete Apache con los módulos php, modss, perl, etc. Sin embargo, no se utilizó esta versión y se instaló Apache 2.0 con la finalidad de poder compilar las librerías

criptográfica gmp y la del manejador de base de datos oci8. Por tanto, si se tiene instalada la versión del sistema debe desinstalarse.

1. Código Fuente: httpd-2.2.3.tar.gz
2. Directorio del Fuente: /usr/src/httpd-2.2.3
3. Compilación como administrador (root)
    a. #./configure –prefix=/usr/local/httpd –enable-so –with-ssl =/usr/local/openssl
    b. # make
    c. # make install
4. Activación del modulo SSL
    a. /usr/local/httpd/conf/vi httpd.conf
    b. Descomentar: `Include conf/extra/httpd-ssl.conf`
5. Cambio de Certificado y llave privada
    a. /usr/local/httpd/conf/extra/vi httpd-ssl.conf
    b. Modificar las líneas:

```
SSLCertificateFile
/usr/local/httpd/conf/votoelectronico.crt

SSLCertificateKeyFile
/usr/local/httpd/conf/votoelectronico.pem
```

6. Abrir el servidor
    a. # /usr/local/httpd/bin/./apachectl start

B.1.3 GMP 4.2.1

1. Código Fuente: gmp-4.2.1.tar.gz
2. Directorio del Fuente: /usr/src/gmp-4.2.1

3. Compilación:
    a. # ./configure –prefix=/usr/local/gmp
    b. # make
    c. # make check
    d. # make install

B.1.4 Oracle 9i

Para la instalación de Oracle, se creó un usuario para la manipulación del software, debido a que como administrador (root) no es posible la apertura de las bases de datos en Linux.

Los pasos de la instalación son los siguientes:

1. Como root, creación de las carpetas para la instalación, creación del usuario y la creación del grupo de trabajo.

    # md /usr/oracle

    # md /usr/oracle/9i

2. Creación de los grupos de trabajo oracle, sysdba y sysoper

    # groupadd sysdba

    # groupadd sysoper

    # groupadd oinstall

    # useradd oracle –d /home/oracle –g oinstall –G sysdba,sysoper

    # passwd oracle

    ****

    # chown oracle.oinstall /usr/oracle

    # chown oracle.oinstall /usr/oracle/9i

3. Configuración del archivo .bash del usuario oracle

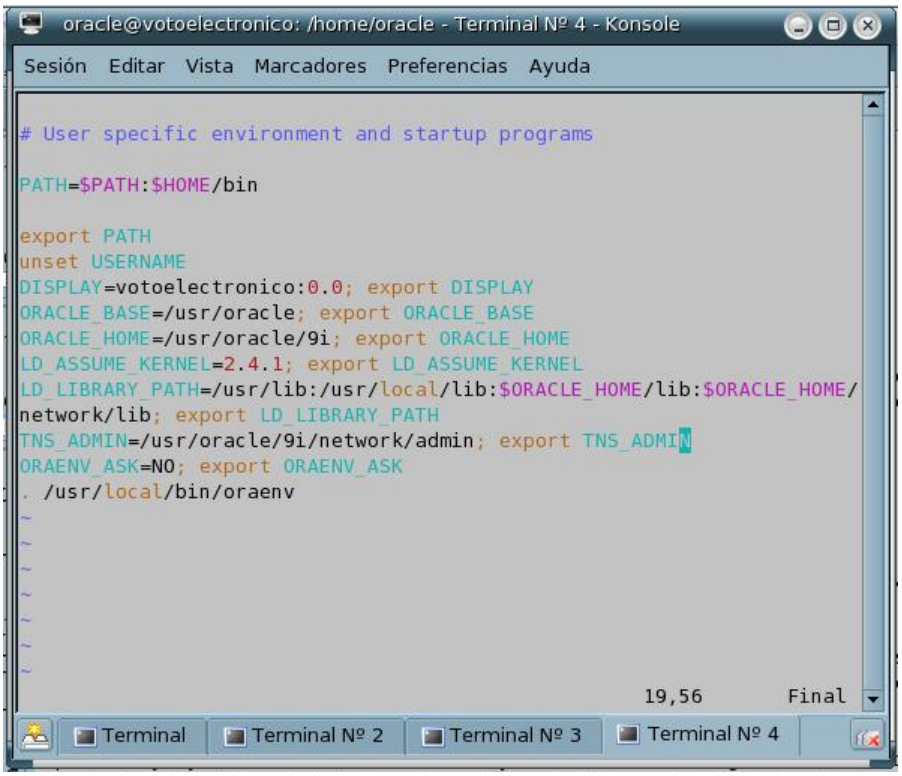


Fig. B.1 Archivo .bash_profile del usuario oracle

4. Abrir sesión del usuario oracle.
5. Copiar los archivos fuente de oracle Disk1, Disk2 y Disk3 en /home/oracle/documents/
6. Ejecutar Disk 1 y seguir el asistente. /home/oracle/documents/Disk1/install/linux/./runInstaller
7. Creación de la Base de Datos. /usr/oracle/9i/bin/./dbca (seguir el asistente)
8. Configuración de la Base de Datos. /usr/oracle/9i/bin/./oemapp console

a. Abrir sesión como sys e ingresar la contraseña indicada en la creación de la base de datos.

b. Creación del tablespace.

c. Creación del usuario administrador de la base de datos.

d. Abrir la sesión del usuario recién creado.

e. Creación de las tablas

9. Activación del Listener para el acceso a la base de datos.

   a. /usr/oracle/9i/bin/./lsnrctl start

10. Apertura de la Base de Datos.

   a. /usr/oracle/9i/bin/.oemapp console

      i. Abrir sesión como usuario administrador.

      ii. Elegir Instancia y abrir la base de datos.

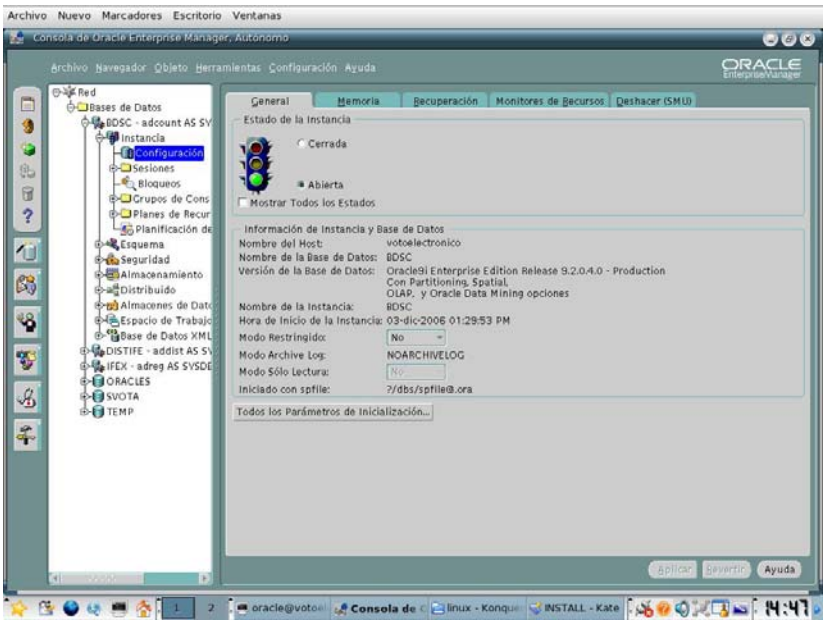


Fig. B.2 Vista del Asistente para la manipulación de la Base de Datos.

Los pasos indicados son los más importantes para la creación y funcionamiento de la base de datos, sin embargo puede abrirse el

puerto para la escucha a las solicitudes de acceso (listener) y a la base de datos de forma automática, para realizarlo consulte el manual de oracle y de linux.

B.1.5 PHP 5.1.4

1. Código Fuente: php-5.1.6.tar.gz
2. Directorio del Fuente: /usr/src/php-5.1.6
3. Compilación:
    a. # ./configure –with-apxs2=/usr/local/httpd/bin/apxs –with-gmp=/usr/src/gmp-4.2.1 –with-oci8=/usr/oracle/9i –with-openssl-dir=/usr/src/openssl-09.8.b
    b. # make
    c. # make install
    d. # cp php.ini-dist /usr/local/lib
4. Configuración del archivo php.ini

    Agregar en el archivo /usr/local/lib/php.ini

    /usr/local/httpd/htdocs/SR/include Para el SR

    /usr/local/httpd/htdocs/SA/includea Para el SA

    /usr/local/httpd/htdocs/SV/includev Para el SV

    /usr/local/httpd/htdocs/SC/includec Para el SC
5. Reapertura del servidor web Apache

    /usr/local/httpd/bin/./apache restart

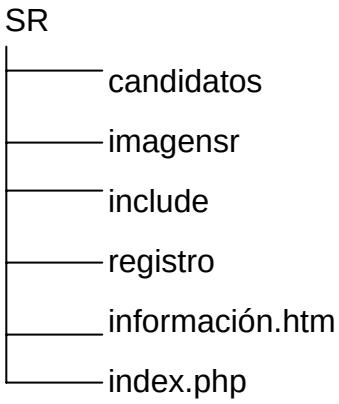
B.2 Código Fuente. SEVI

El código de SEVI está divido en sus cuatro servidores, las carpetas principales son SR, SA, SV y SC para cada servidor.

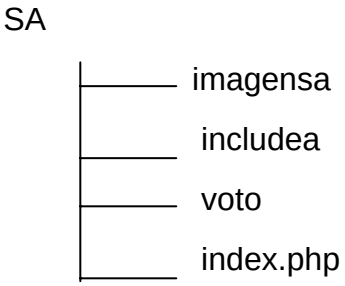
Para el uso de los servidores basta con configurar cada uno con las instrucciones de la sección anterior y copiar la carpeta respectiva a cada servidor en la carpeta /usr/local/httpd/htdocs.

A continuación se presentan los árboles de carpetas contenidas para cada servidor sólo a manera de ilustración.

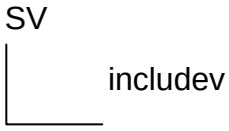
Servidor de Registro (SR)



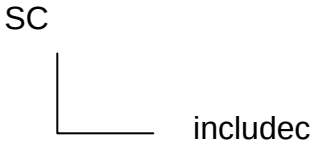
Servidor de Autenticación (SA)



Servidor de Votación (SV)



Servidor de Conteo (SC)



Bibliografía

[1] Instituto Federal Electoral, “Código Federal de Instituciones y Procedimientos Electorales” (COFIPE), 2005. http://www.ife.org.mx

[2] Instituto Federal Electoral, “Voto en el Extranjero” 2006. http://www.ife.org.mx

[3] F. Robles Nava, “No garantizan el voto mexicano por correo”, Nota de la Opinión, 28 de mayo 2005.

[4] California Internet Voting Task Force, “A Report on the Feasibility of Internet Voting”, Jan 2000. http://www.ss.ca.gov/executive/ivote/.

[5] Instituto Electoral y de Participación Ciudadana de Coahuila (IEPCC), “Voto Extraterritorial”, 2004. http://www.iepcc.org.mx/ademocracia/a01.html

[6] C. García, F. Rodríguez, “Sistema Electrónico para Elecciones Seguras (SELES)”, Tesis Maestría, Cinvestav-IPN, México, DF. Sep. 2005.
http://delta.cs.cinvestav.mx/~francisco/ssi2005/ssi05.html

[7] I. Lin, M. Hwang and C. Chang, “Security enhancement for anonymous secure e-voting over a network”, Computer Standards & Interfaces, Vol. 25, Issue 2, pages: 131-139, 2003.

[8] F. Rodríguez-Henríquez, D. Ortiz-Arroyo and C. García-Zamora, “Yet Another Improvement over the Mu-Varadharajan e-voting Protocol”, The Journal of Computer Standards and Interfaces, Elsevier, 2007.

[9] I. Jacobson, G. Booch and J. Rumbaugh, “El Proceso Unificado de Desarrollo de Software”, Addison Wesley, 2000.

[10] I. Jacobson, G. Booch and J. Rumbaugh, “El Lenguaje Unificado de Modelado”, Addison Wesley, 2000.

[11] D. Chaum, “Secret-Ballot Receipts: True Voter-Verifiable Elections”, Security & Privacy Magazine, IEEE Vol. 2, Issue 1, pages 38-47, Jan-Feb 2004.

[12] ACM TechNews. http://technews.acm.org

[13] B. Schneier, “Voting Security and Technology”, Security & Privacy Magazine, IEEE July-Ago 2004.

[14] J. Bannet, D.W. Price, J. Singer and D.S. Wallach, “Hack a Vote: Security Issues with Electronic Voting Systems”, Security & Privacy Magazine, IEEE Vol. 2, Issue 1, Jan-Feb 2004.

[15] B. Simons, "Electronic Voting Systems: the Good, the Bad and the Stupid”, ACM Queued Vol.2 Issue 7, Oct. 2004.

[16] D. Evans and N. Paul, “Election security: Perception and reality”, Security & Privacy Magazine, IEEE Vol. 2, Issue 1, pages 24 – 31, Jan-Feb 2004.

[17] A. Di Franco, A. Petro, E. Shear and V. Vladimirov, “Small vote manipulations can swing elections”, Communications of the ACM, Vol. 47, Issue 10, page 43-45, Oct. 2004.

[18] J. Kitcak, “Source Availability and e-voting: an advocate recants”, Communications of the ACM, Vol. 47, Issue 10, pages 65-67, Oct. 2004

[19] J. Grove, “ACM statement on voting systems”, Comunications of the ACM 950:69-70, 2004.

[20] L. López y M. A. León, “Sistema de Votación por Internet para la Elección de Presidente de México”, 4th Congreso Nacional en Ciencias de la Computación, Puebla, México, 2006.

[21] National Science Foundation, “Report on the National Workshop on Internet Voting: Issues and Research Agenda”, March 2001.

[22] D. Jefferson, A. D. Rubin, B. Simons and D. Wagner, “A Security Analysis of the Secure Electronic Registration and Voting (SERVE)”, 2004. http://www.servesecurityreport.org.

[23] Gaceta Parlamentaria, Año VII, Número 1522 http://www.reformadelestado.gob.mx

[24] W. Trappe and L.C. Washington, “Introduction to Cryptography with Coding Theory”, Prentice Hall, pages 60-9, 2002.

[25] F. J. Hirsch, “Introducing SSL and Certificate using SSLeay”, Web Security: A Matter or Trust, World Wide Web Journal, Vol. 2, Issue 3, Summer 1997.

[26] J. C. Orós, “Diseño de Páginas Web Interactivos con JavaScript”, Alfaomega Ra-Ma.

[27] S. Bobrowski, “ORACLE 8i para Linux”, Edición de Aprendizaje, McGraw-Hill.

[28] C. Pérez, “Oracle 9i Administración y Análisis de Bases de Datos”, Alfaomega Ra-Ma.

[29] J. Valade, “PHP 5 para Dummies”, ST Editorial.

[30] A. Gutiérrez y G. Bravo, “PHP 4 a través de Ejemplos”, Alfaomega Ra-Ma.

[31] A.J. Stieber, “OpenSSL Hacks”, Linux Journal, July 2006. http://www.linuxjournal.com/article/8958